UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

HISCOX INSURANCE COMPANY, INC. and HISCOX SYNDICATES LIMITED Plaintiffs, vs. WARDEN GRIER, LLP Defendant.	)	Case No. 4:20-cv-00237-NKL

PLAINTIFFS HISCOX COMPANY, INC. AND HISCOX SYNDICATES LIMITED'S SUGGESTIONS IN OPPOSITION TO DEFENDANT WARDEN GRIER, LLP'S MOTION FOR SUMMARY JUDGMENT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

RESPONSE TO STATEMENT OF UNCONTROVERTED MATERIAL FACTS

1. Warden Grier is a Limited Liability Partnership with 4 attorneys.

    a. James (Jim) Warden has been practicing since 1975 and is AV rated.

    b. Michael (Mike) Grier has been practicing since 1984 and is AV rated.

    c. Kristopher (Kris) Kuehn has been practicing since 1989 and is AV rated.

(*James M. Warden Affidavit*, ¶¶ 1, 2)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. Warden Grier's organizational structure and the experience and AV ratings of its attorneys are immaterial to Hiscox's claims or to any issue raised in Warden Grier's motion.

2. Warden Grier has an ongoing relationship with Hiscox. (*Warden Affidavit*, ¶ 3)

    a. Hiscox Insurance Company Inc. is an Illinois corporation with its principal place of business in Chicago, Illinois. Hiscox Syndicates Limited is a private limited company formed under the laws of England and Wales. Its principal place of business is in London, England. (*Complaint*, ¶¶ 1, 2)

    b. Hiscox is an insurance provider that insures risks throughout the United States and retains service providers, such as law firms, to represent its interests or its insureds. (*Complaint*, ¶ 6)

    c. Hiscox entered into a working relationship with Warden Grier, as early as 2002, to render professional legal services. (*Complaint*, ¶ 7)

    d. The relationship between Hiscox and Warden Grier was memorialized and governed, in part, by two separate contracts. (*Complaint*, ¶ 8)

    e. Both contracts contain the following language: "You will not normally make a charge for the cost of retrieving retained documents or property in response to continuing or new instructions from us. You may, however, make a charge based upon time spent in reviewing documents or undertaking other work necessary to comply with our instructions." (Depo. Ex. 2, p. 10; Depo. Ex. 3, p. 9)

    f. Warden Grier represented Hiscox in coverage matters, subrogation matters and monitoring Hiscox litigation in the United States. (*Warden Affidavit*, ¶ 3)

    g. Warden Grier may have represented Hiscox's insureds in a few matters prior to 2008, but none by 2016, 2017 or 2018. (*Warden Affidavit*, ¶ 3)

RESPONSE: OBJECTION that the statement fails to comply with Local Rule 56.1(a). The statement does not comply with Local Rule 56.1(a) because it includes numerous facts in multiple, unrelated subparagraphs rather than placing each fact in a separately numbered paragraph.

Subject to that objection, the statement is CONTROVERTED inasmuch as the phrase "ongoing relationship" means Hiscox continues to hire Warden Grier for legal work. Witnesses testified "the relationship had stopped" and Hiscox ceased hiring Warden Grier for legal work. The evidence suggests that continuing representation, if any, was a result of the Lloyd's of London system and involved instances when Hiscox was a secondary participant and/or when another entity directed the work. *See, e.g.*, Ex. 1 (Warden Dep.) at 56:20-58:23; Ex. 2 (Pinchin Dep., Vol. II) at 151:22-152:14.

3. Warden Grier discovered on February 14, 2017 their server had been hacked by an international hacker organization known as the "The Dark Overlord" (TDO). (*Warden Affidavit*, ¶ 4)

RESPONSE: ADMITTED for purposes of this motion.

4. Hiscox does not claim that Warden Grier was negligent or breached a fiduciary duty in allowing the data breach to occur or in its data security practices, policies or procedures. Nor is Hiscox pursuing breach of contract or implied contract claims. (Depo. Ex. 11)

RESPONSE: ADMITTED for purposes of this motion.

5. Warden Grier knew the cases they had, the clients they had and therefore knew in a general sense and to a great extent a detailed sense the type of information on the compromised server. David Chronister of Parameter gave Warden Grier oral reports of what was on the server and Warden Grier also looked at the indices the hacker provided in the link. (*Warden Affidavit*, ¶ 5b-d) (WGR000379 – Transmittal of Image File Listing)

RESPONSE: CONTROVERTED that Warden Grier had a "detailed sense [of] the type of information on the compromised served."

As explained more in the accompanying suggestions, after a review of the record Hiscox's expert witness testified that Warden Grier failed to take reasonable steps to understand the nature of the impacted data, including analyzing the data for PII and identifying the affected individuals and their states of residency. *See, e.g.*, Ex. 3

(Worley Report). Warden Grier's outside attorney likewise advised the law firm to review the data to (1) determine which individuals' PII was compromised, (2) confirm their residency, and then (3) review the requirements based upon the applicable states' laws. *See* Ex. 4 (Dep. Ex. 112) at 1.

Warden Grier did not undertake this analysis and instead relied upon its attorney's recollections and general assumptions, including Jim Warden's belief that "there might be some medical information on the server . . . other types of information like SSNs could [also] be present" but that this information was "very limited" and "at least one to two and a half years old." Ex. 3 (Worley Report) §§ 47-48, Ex. 1 (Warden Dep.) at 104:20-107:9. Warden Grier also refused to do any searching or checking to determine whose PII might be on the affected server. Ex. 1 (Warden Dep.) at 106:22-25.

As it turned out, Warden Grier was incorrect in its belief that the PII was "very limited" or "at least one to two and half years old." In fact, the server contained PII of around 8,500 people in Hiscox's files alone. Ex. 3 (Worley Report) ¶ 80; Ex. 5 (HIC005502) at 5503. And the server included active case files, including a database Warden Grier used in its work monitoring cases filed against insured nursing homes. Ex. 6 (Murphy Report) ¶ 13(b) & Ex. C attached thereto; Ex. 7 (Kuehn Dep.) at 31:4-32:13, 42:13-19, 47:10-48:7. If, as it contends in this statement, Warden Grier had a "detailed sense the type of information on the compromised server" it would not have concluded incorrectly that the PII was "very limited" or "at least one to two and half years old."

6. Hiscox was aware that Warden Grier had PII that had been provided by Hiscox.

Q. Okay. Do you know if during the time that Warden Grier was doing work for Hiscox, were they ever provided any personal identifiable information from Hiscox to that law firm?

A. I repeat that I am not responsible for the day-to-day conduct of that relationship, but as I would understand, in order to fulfill their role and the work, it would necessarily involve the provision of PII. (*Pinchin*, p. 24)

<u>RESPONSE</u>: ADMITTED for purposes of this motion but IMMATERIAL. Whether Hiscox "was aware" that it provided PII to Hiscox is immaterial to Hiscox's claims or to any issue raised in Warden Grier's motion.

7. Hiscox itself has no PII and is not a covered entity for HIPPA purposes.

Q. And I understand that individuals have PII, and a corporation may be collecting that and have it. But the corporation itself doesn't have PII?

A. That is correct, yes.

Q. All right.

A. So PII is personally identifiable information relating to an identified or identifiable living human. (*Worley*, p. 205)

…

Q. Was Hiscox a covered entity in this particular data breach?

A. I do not think so. That's not something I analyzed, but they're not a healthcare provider, a clearinghouse -- I'm trying to think of what else - or continuing with healthcare. So no, they wouldn't be a covered entity. (*Worley*, p. 71)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, whether Hiscox has PII of its own or is a HIPAA covered entity is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

8. The Warden Grier data breach may have included information relating to 1,500 of Hiscox's commercial policyholders. (Depo. Ex. 27)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) that the cited material does not support the factual statement. The referenced document reflects Hiscox's belief about the potential scope of the data breach in April 2018, shortly after having learned about the breach and before anyone reviewed the underlying data. Further, the statement misrepresents the cited document, which states the server may have included information relating to "up to" 1,500 of Hiscox's commercial policyholders.

Subject to that objection, the statement is ADMITTED for purposes of this motion.

9. Hiscox commercial policyholders were not individuals. PII only applies to individuals, not Hiscox's commercial entities. (*Walter*, p. 73) (*Kam*, p. 52)

Q. (By Mr. Horn) Okay. The information that was going to be disclosed could have been harmful to your policyholders who are your customers, correct?

A. In this case, the PII, as you referred to before, wasn't really our policyholders. It was customers of our policyholders.

Q. So you're saying there wasn't any PII of your actual policyholders?

A. Our policyholders are not individuals and -- in this case, and PII only applies to individuals, not to commercial entities. (*Walter*, p. 73)

…

Q. What individuals did Hiscox notify?

A. I do not recall exactly.

Q. And are you distinguishing between individuals and policyholders?

A. Yes.

Q. And when you use the term individual, what are you referring to?

A. I'm referring to individuals where the PII belongs to them. We have policyholders that are organizations or companies, so they're not actually individuals.

Q. And so --

A. They wouldn't have -- a company wouldn't have PII on its own.

Q. Right.
Just like Hiscox doesn't have PII on its own?

A. Yeah (*Kam*, p. 52).

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, whether Hiscox's policyholders have PII of their own is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law. For reasons explained in the accompanying suggestions, Hiscox still had notice obligations to its corporate policyholders resulting from the unauthorized access to PII.

10. Upon learning of the hack, Warden Grier sought advice and counsel from computer professionals, legal professionals, and the FBI. (*Warden Affidavit*, ¶ 5)

RESPONSE: ADMITTED for purposes of this motion.

11. The computer professionals were Cytek and Parameter. (*Warden Affidavit*, ¶ 5a, 5c)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. The identities of Warden Grier's computer professionals are immaterial to Hiscox's claims or to any issue raised in Warden Grier's motion.

12. The legal professionals were Peter Sloan and Jeff Jensen. (*Warden Affidavit*, ¶ 5b, 5e)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

13. The FBI liaison and former agent was Chris Budke; two active FBI agents were also involved. (*Warden Affidavit*, 5e, 5f)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

14. The Dark Overlord threatened to publicize all data they had copied off the Warden Grier server unless Warden Grier paid a ransom.

a. "Well, let's start with what's going to happen if you don't comply with our demands. If you ignore us or otherwise fail to comply, we're going to bring the media into this breach. We're going to publicly leak every single document and case file your firm (and that other pesky firm some of you came from) that you've ever created." (Depo. Ex. 124)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As discussed in the accompanying suggestions, Warden Grier's decision about whether to pay ransom is irrelevant and immaterial to Hiscox's claims that Warden Grier committed professional negligence and breached its fiduciary duties in failing to analyze the compromised data for PII or notify clients about the breach.

15. Warden Grier and Budke were informed by the FBI that in 23 of 24 cases when the TDO was not paid a ransom they had publicized the stolen data. In the case where the ransom was paid, the information was not made public. (*Warden Affidavit*, ¶ 6)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) that Warden Grier cannot support the facts about the purported other cases and, in particular, its factual statement that "[i]n the case where the ransom was paid, the information was not made public" with admissible evidence. The affiant has no personal knowledge of the other alleged instances. And the out-of-court statements of the FBI are inadmissible hearsay.

Subject to that objection, the statement is ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Warden Grier's decision about whether to pay a ransom is irrelevant and immaterial to Hiscox's claims that Warden Grier committed professional negligence and breached its fiduciary duties in failing to analyze the compromised data for PII or notify clients about the breach.

16. Warden Grier agreed to pay the ransom (50 bitcoin) in order to prevent its clients' data from being made public. (*Warden Affidavit*, ¶ 7)

RESPONSE: CONTROVERTED that Warden Grier agreed to pay the ransom "to prevent its clients' data from being made public." There is evidence from which a jury could infer that Warden Grier paid the ransom to keep the data breach secret and to protect its own interests, including its interests in avoiding the negative impacts of making breach notifications and financial consequences of having to review the data for PII. *See, e.g.*, Ex. 8 (Dep. Ex. 133) (Warden Grier statement that "[w]e might have wasted $60k [the ransom] as it appears to me we are headed back toward [client] disclosure"); Ex. 9 (Dep. Ex. 120) at 2322 (Warden Grier statement about shutting down Kansas entity to "keep value of future work and distance ourselves from this bottomless pit of expense").

17. Hiscox's retained expert, Worley, agreed that Warden Grier chose to pay the ransom to the hacker as part of its obligation to protect clients and that it was in the clients' interest to have the information that was in the hands of the bad guy destroyed.

Q. And in it, they say, We're going to publicly leak every single document and case file your firm -- that you've ever created. Do you see that?

A. Yes.

Q. Do you believe Warden Grier was acting in their clients' best interest to try to prevent that from happening?

A. I believe that Warden Grier had an obligation to act in their clients' best interest, and part of that analysis could be the publication of these materials.

Q. And part of that analysis would be the decision to pay the ransom in order to keep this from happening?

A. They needed to consider the nature of the data, the risk to individuals to whom the data belonged, their regulatory obligations, the regulatory obligations of their clients, and their status as fiduciaries.

Q. And having considered that, in paying the ransom, do you believe they were trying to look out for the best interest of their clients?

A. I think that was probably one of their considerations. (*Worley*, p. 184-185)

…

Q. That would be -- it would be in their clients' interest to have the information that was in the hands of the bad guy destroyed, if that could be done?

A. Yes, I agree with that. (*Worley*, p. 83)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) that the cited material does not support the factual statement. The cited testimony does not state that Warden Grier paid the ransom "as part of its obligation to protect clients." It says "I think that [looking out for the best interest of their clients] was probably one of their considerations." *See* portions of transcript cited above.

Subject to that objection, the statement is CONTROVERTED. *See* portions of transcript cited above.

18. Warden Grier paid the Hackers a ransom or other demand to protect its and its clients' personal information from dissemination. (*Complaint*, ¶ 15)

RESPONSE: CONTROVERTED. Although this statement accurately quotes paragraph 15 of the complaint Hiscox filed in March 2020, there is evidence from which a jury could infer that Warden Grier paid the ransom not to protect its and its clients' personal information from dissemination but to keep the data breach secret and to protect Warden Grier's own interests, including its interests in avoiding the negative impacts of making breach notifications and financial consequences of having to review the data for PII. *See, e.g.*, Ex. 8 (Dep. Ex. 133) (Warden Grier statement that "[w]e might have wasted $60k [the ransom] as it appears to me we are headed back toward [client] disclosure"); Ex. 9 (Dep. Ex. 120) at 2322 (Warden Grier statement about shutting down Kansas entity to "keep value of future work and distance ourselves from this bottomless pit of expense").

19. Warden Grier did not inform their clients of the hack in 2017 because the TDO threatened to disclose the data if they did so. They agreed to destroy the data if the ransom was paid.

> Condition B is that the "Client" or other associated parties of the "Client" will refrain from communicating in any method, design, or otherwise to any computer, corporation, individual person or other entity any knowledge, information, or otherwise about this agreement.
>
> Conditionally, the "Proposer" will securely destroy all copies of the "Client's" or other associated parties of the "Client's" "data' and the "Proposer" promises that no part of any of the "Client's" data or any information about this incident has been shared with any non "public' computer, corporation, individual, person, or other entity. (Depo. Ex. 131)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) that the cited material does not support the factual statement about Warden Grier's reasons for not informing their clients of the hack in 2017. The cited material merely recites provisions of an alleged "contract" between Warden Grier and the hackers. Even if the contract was enforceable, its provisions do not bar Warden Grier from notifying clients or other affected individuals of the data breach in 2017 after having paid ransom. *See* Doc. 89-12.

Subject to that objection, the statement is CONTROVERTED. Warden Grier still could have informed its clients of the hack in 2017 after having paid the ransom and after the hackers were supposed to have deleted the data. *See* Ex. 10 (Worley Dep.) at 77:14-19 ("Generally, in cases like this, where we know there's been exfiltration, you pay the ransom to buy time, to try to protect the data while you are doing the other analysis, which is figuring out what data was impacted and what regulations apply"); *see also id.* at 76:12-80:14; Ex. 1 (Warden Dep.) at 133:17-134:8; Ex. 11 (Downey Dep.) at 45:3-50:15.

20. Warden Grier documented their actions and decisions in a Memorandum dated February 27, 2017. (Depo. Ex. 115, 116).

RESPONSE: ADMITTED for purposes of this motion.

21. Warden Grier's legal adviser, Peter Sloan, agreed that Hiscox did not need to be notified in 2017.

a. "My belief and opinion that under the circumstances of this matter, Warden Grier met its obligations to Hiscox in 2017, and that in my view, Warden Grier's decision on the handling of the circumstances of this event between the spring of 2017 and the end of March 2018 in my view was appropriate." (*Sloan*, p. 6)

b. "It's my understanding they made the determination [not to notify clients] and I happen to agree with that determination in the circumstances of this accident." (*Sloan*, p. 71)

c. "I reviewed the draft memo from Jim Warden that captured that decision and reasons for it, I thought about it, I had not before and did not then tell Warden Grier what they needed to do or what they should do or what they had to do. That was a decision for them to make. What I'm saying is based on the circumstances, the particular circumstances of this matter and of this event, I truly believe that Warden Grier met its obligations to its clients and, in fact, I think acted admirably - - I think that's word I use in my report because I truly believe that – met its obligations to its clients in not disclosing this event prior to late March 2018." (*Sloan*, p. 99-100)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) and MOVE TO STRIKE.

Sloan's opinion that Warden Grier met its obligations to Hiscox in 2017 or acted appropriately or "admirably" is inadmissible because Sloan is a retained expert who did not disclose the opinion in his expert report. The report includes this opinion only in a footnote and without further elaboration. *See* Ex. 12 (Sloan Report) at 7 n.1. Such disclosure does not fulfill Rule 26(a)(2)(B)'s requirement "that an expert's report include the 'basis and reasons' for his opinions in addition to including the 'the data or other information considered by the witness in forming the opinions.'" *See Nat'l Union Fire Ins. Co. of Pittsburgh v. Midwestern Gen. Brokerage, Inc.*, No. 06-0782-NKL, 2007 WL 1529011, (W.D. Mo. May 23, 2007) (striking expert's standard-of-care opinion for same reason).

Further, Sloan's testimony is not admissible as fact testimony. Among other reasons, (1) Sloan claims to have formed the opinion only after the fact and not to have communicated this information to Warden Grier (*see* Ex. 13 (Sloan Dep.) at 99:13-100:2), and (2) Sloan was Warden Grier's lawyer in 2017 and Warden Grier waived an advice of counsel defense in this case (*see* Ex. 14 (Resp. to Interrog. No. 4)).

22. The Cooley law firm provided Hiscox talking points with WG as well as the underlying legal analysis supporting those positions. Cooley wrote:

> Ethical/Moral Considerations – Attorney-Client Relationship
>
> Lawyers in the U.S. must abide by the Rules of Professional Conduct. While these do not require any notification following a breach, they do require lawyers generally to act in an ethical manner and zealously represent their clients.
>
> Client agreements/engagement letters may have confidentiality provisions or other notice requirements in the event of a security incident affecting client data or of disclosure to third parties without consent. (Depo. Ex. 79)

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the cited document but CONTROVERTED that the Rules of Professional Conduct do not require notification following a breach. *See generally* Ex. 3 (Worley Report); *see also* Ex. 15 (Navetta Dep.) at 74:19-24 ("There are no specific breach notification laws for lawyers. That's what I think was the content, but there may be ethical issues that require some sort of addressing of a confidentiality breach like this.").

23. Hiscox has in other situations, for its cyber insurance policyholders, agreed to pay a ransom for the insured in order to have the insured's information returned or destroyed by the hacker.

Q. And does Hiscox cyber policies that you were involved in pay for ransom payments to unauthorized individuals?

A. Yes.

Q. Did you ever have those situations where you were involved in that, where a ransom was paid to the unauthorized hackers?

A. Yes.

Q. Can you tell me generally about situations you were involved in which Hiscox paid a ransom to the unauthorized individuals who had hacked into a policyholder's computer system?

A. About the situation generally or the process? What exactly are you asking?

Q. Tell me about the situation generally.

A. If a policyholder had received a ransom demand and it was covered under their policy and there was no other way for them to recover their data that had been encrypted then Hiscox would engage a vendor to negotiate with the threat actor and pay the ransom on behalf of the insured (*Yung*, p. 14-15)

…

Q. Would there be also times where the unauthorized hacker claimed that they had obtained information from the policyholder that they were not going to give back unless a ransom had been paid?

A. Yes.

Q. So, you understand there's kind of two situations then, you can have ransom paid in order to get your systems operating again, you understand that type of ransom?

A. Yes.

Q. And I think we've seen that in the news here recently with the pipeline situation and some other situations, that the computer systems were essentially frozen until a ransom was paid. So, you understand that type?

A. Yes.

Q. The other type is where the hacker has claimed to have taken certain information from the policyholder and is threatening to release it or use it unless a ransom is paid?

A. Yes.

Q. And you've dealt with both those situations for Hiscox?

A. Yes.

Q. And when those situations occur, as I understand it, Hiscox has a list of approved vendors that will negotiate the ransom payments?

A. Yes.

Q. And in the situations where the ransom payments have been paid by Hiscox on behalf of their policyholders what has been the result?

A. What do you mean by that?

Q. Has the result been, when the ransom is paid have the hackers then freed up the policyholder's computer systems as promised?

A. Usually, yes.

Q. And in situations where the hackers claim to have had information stolen from the policyholder, when the ransom is paid has that information either been returned or destroyed by the hackers?

A. Usually, yes.

Q. When you say usually, has it happened that the ransom is sometimes paid and the criminals/hackers do not stick to their promise?

A. It's not necessarily that they don't stick to their promise, it's because we don't have a direct line to the hackers and it's hard to tell with a hundred percent certainty whether they deleted it like they say they did. There's no way to know with certainty.

Q. Have there been situations where they promised to delete account information but you found out later they did not?

A. Not to my knowledge.

Q. So, in the situations where the criminal hackers made a promise to delete the information if the ransom is paid, the assumption is that they did do that, you just can't know that with a hundred percent certainty?

A. That's my understanding, yes.

Q. And you're not aware of any situation that you handled where later, after the ransom has been paid to the criminal hackers, they in fact release the information?

A. Not after the fact, no. (*Yung*, p. 16-18)

…

Q. So sometimes would Hiscox agree to pay a ransom on behalf of their insured in order to keep from having divulged sensitive or proprietary information

A. That could happen, yes.

Q. And has that been done in the past by Hiscox?

A. I'm sure it has. (*Walter*, p. 17-18)

…

Q. No. I understand that. But I'm talking specifically about the threat where the criminal, the bad actor says unless you pay us a certain ransom, we are going to divulge that information publicly. I'm talking specifically about that type of threat. Okay?

A. Okay.

Q. And in that situation, does Hiscox at times recommend that the ransom be paid in order to keep that from happening?

A. At times.

Q. And that has, in fact, happened in the past where Hiscox has paid on behalf of their insurer ransom in order to keep the information from being made public?

A. We -- we typically would not make that payment, but we would reimburse the clients for those expenses under the terms of their insurance contract. (*Walter*, p. 23)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As discussed in the accompanying suggestions, the decision about whether to pay a ransom is irrelevant and immaterial to Hiscox's claims that Warden Grier committed professional negligence and breached its fiduciary duties in failing to analyze the compromised data for PII or notify clients about the breach.

24. Hiscox's U.S. CEO, Ben Walter, testified that the Warden Grier payment of the ransom likely prevented the public disclosure of the information that had been stolen from their server.

Q. Do you have an opinion that, by paying the ransom, Warden Grier prevented the public disclosure of this information that had been stolen from their server?

A. I think that's likely true. (Walter p. 135)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As discussed in the accompanying suggestions, the decision about whether to pay a ransom is irrelevant and immaterial to Hiscox's claims that Warden Grier committed professional negligence and breached its fiduciary duties in failing to analyze the compromised data for PII or notify clients about the breach.

25. In the Spring of 2018 the TDO accused Warden Grier of cooperating with the FBI and threatened to release some of the data they had stolen but had not destroyed unless they were paid an additional ransom. (Depo. Ex. 135, 139)

RESPONSE: ADMITTED for purposes of this motion.

26. Warden Grier consulted with Sloan and the FBI concerning this new threat. Warden Grier tried to determine if it was a legitimate threat or if the criminals could produce any evidence that they actually had anything. (*Warden Affidavit*, ¶ 9)

RESPONSE: ADMITTED for purposes of this motion.

27. Hiscox's outside attorney, Navetta, wrote that the attackers "had this data for more than 18 months, and nothing has come out except a vague tweet referring to Hiscox and Lloyd's threatening release of supposed embarrassing information, which then never occurred." (Depo. Ex. 54)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

28. On March 29, 2018, TDO informed Warden Grier they had notified Hiscox of the breach and threatened to kill Mike Grier. (Depo. Ex. 140)

RESPONSE: ADMITTED for purposes of this motion.

29. Hiscox contacted Warden Grier on March 31, 2018, and Warden Grier confirmed they had been hacked by the TDO. (Depo. Ex. 141, 142, 143)

RESPONSE: ADMITTED for purposes of this motion.

30. Ben Walter, CEO of Hiscox U.S., testified the delay from the time Warden Grier knew of the hack (Feb. 14, 2017) until Hiscox learned of the hack (March 29, 2018) had no direct result in terms of what had to be done. If Hiscox had been informed a year earlier the same investigation would have had to occur.

> Q. And there was approximately a 15-month delay between the time that Warden Grier became aware of the criminal hack and Hiscox became aware of the criminal hack, correct?
>
> A. If the date of December is correct, then yes.
>
> Q. And so the delay of 15 months, tell me what -- what were the results for Hiscox that there had been a delay of 15 months?
>
> A. The result -- the direct result was -- in terms of what had to be done was nothing. We had to do the same things we would have had to do or that we would have expected Warden Grier to do. Those were all the same. It was just delayed and we didn't know about it. (Walter p. 60)
>
> …
>
> Q. So if you had been informed a year earlier, the same investigation would have had to have occurred?
>
> A. Yes.
>
> Q. And you would have had a discussion then with Warden Grier about who's going to pay for the investigation?
>
> A. We might have. I don't know. (Walter p. 86)

Likewise, Jeremy Pinchin, Hiscox Group Head of Claims, testified that Hiscox would have taken the same steps if it had been notified 2 years earlier. (Pinchin p. 110 and 112).

> Q. And if you had been told that a year earlier, what would you have done?
>
> A. We would have immediately sought advice, as we did, from specialist U.S. attorneys on our legal obligations to our insureds and our reporting obligations to regulatory authorities.
>
> Q. Which is what you ultimately did?

A. It is. (Pinchin p. 110)

…

A. We took very immediate steps to act in the best way we could to protect our clients some two years after the hack had taken place because we hadn't been informed by Warden Grier of it. I am aware of absolutely no delays whatsoever in the process of notification, other than the complexity of undertaking the role and ensuring that we did it in a proper fair manner.

Q. (By Mr. Horn) You would have taken those same steps a year earlier, correct?

A. We would have taken those same steps in accordance with advice two years earlier. (Pinchin p. 112)

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witnesses' testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

31. Tara Bodden, Hiscox's Senior Claims Counsel, testified that Hiscox would have wanted its data that had been hacked and would have done its own investigation even if they had been notified in February 2017. (Bodden p. 57-64).

Q. So, when the -- when you learn about this and the data goes to Charles River Associates, I take it Hiscox wants to know what data of theirs was on the compromised server that may now be in the hands of cyber criminals, right? (Bodden p. 58)

Q. That's the first thing you have to do, correct?

A. Yes.

Q. Try to figure out what the cyber criminals have of the Hiscox data, correct?

A. That's -- yes. (Bodden p. 58-59)

…

Q. And that step one for Hiscox is, give us the data that they might have seen or they have -

A. That's correct.

Q. -- so that we can figure out what we need to do, right?

A. Yes.

Q. Because as an insurance company and subject to different regulations and all you have certain legal obligations that are specific to an insurance company operating in the United States that may be completely separate from Warden Grier's obligations after a data breach?

A. That's true, yes.

Q. So, you need to see your data to figure out what we need to do?

A. Yes, we need to understand what documents and information may have been improperly accessed.

Q. You would need to know that in 2017 or 2018, you need to know it whenever you learn of the breach, correct?

A. That's correct.

Q. So, if the day after Warden Grier gets a nasty e-mail from the dark overlord saying, we breached your systems, if Warden Grier had called Hiscox the next day and said, our systems have been breached, Hiscox would want to know what data is possibly on your system that they have seen or now have?

A. Yes.

Q. And then you would have wanted to say, give us that data so we can figure out what our legal obligations are?

MR. SEITZ: Objection, incomplete hypothetical, vague as to time period.

Q. In 2017, the day after Warden Grier learned for the first time that their server had been compromised, that's the time period I'm talking about now.

MR. SEITZ: Objection, incomplete hypothetical. Go ahead.

THE WITNESS: Just repeat your question. I'm sorry.

BY MR. HORN:

Q. Warden Grier learns of the hack in February of 2017.

A. Yes.

Q. The next day they call up Hiscox and say, our server is hacked, they may have seen and they may have everything involving Hiscox on the server. Okay?

Follow me?

A. Uh-huh.

Q. Right?

A. Yes.

Q. You would have told Warden Grier, give us the data that they either have seen or they might have?

MR. SEITZ: Objection. Incomplete

Hypothetical, calls for speculation, assumes facts not in evidence.

Go ahead.

THE WITNESS: Yes, we would have wanted to know what that information was.

Q. Right. That's step one for Hiscox?

MR. SEITZ: Same objections.

BY MR. HORN:

Q. Correct?

A. Yes. (Bodden p. 60-63)

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witness's testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

32. Bodden testified that after Hiscox gets the data they hire Cooley (law firm) and Charles River Associates (CRA) to analyze the data to figure out what Hiscox's legal obligations are. (Bodden p. 57-64) and based on the analysis Hiscox sends out notices to whoever Hiscox believes they are required to by law and inform any regulators Hiscox believes they are obligated to inform. (Bodden p. 64)

Q. And so, whether it was in 2017 when the breach occurred to Warden Grier's knowledge, or 2018 when Hiscox learned of the breach, once you learn of the breach Hiscox has certain legal obligations that it has to follow?

A. Yes.

Q. And those obligations are for Hiscox to do an investigation to determine what they have to do under the privacy regulations?

A. Yes.

Q. And Hiscox does some of that perhaps internally, but they then hire a law firm like Cooley to advise them what are our obligations now that we know of the breach? (Bodden p. 57)

…

A. Yes.

Q. And then you hire someone like Charles River Associates to look at the data to figure out how that plays into what Hiscox's obligations are with regards to the breach?

THE WITNESS: Yes.

Q. And then when all that's done Hiscox sits down with their lawyer and determines, here's now who we need to notify as a result of this breach, be it individuals, policyholders or regulators?

A. That's correct.

Q. And then Hiscox determines, with its lawyers, what that notification will look like?

A. That's correct. The lawyers generally, the breach counsel say this is what it needs to look like.

Q. At the same time, Warden Grier may have their own obligations with regards to the breach as to notifying individuals or other clients?

A. Presumably, yes. (Bodden p. 58)

Q. Right. But if they tell you it has Hiscox data on it you want to see the data?

MR. SEITZ: Same objections.

THE WITNESS: Correct.

Q. Okay. And then you take that data, and along with a law firm you hire like Cooley and Charles River Associates, you analyze the data to figure out what are our legal obligations now that the cyber criminals have seen it or have it?

MR. SEITZ: Objection, assumes facts not in evidence, incomplete hypothetical, calls for speculation.

Go ahead.

BY MR. HORN:

Q. Correct?

A. Yes.

Q. Then based upon that analysis you send out notifications to whoever you believe you're required to do that by law, right?

A. That's correct, yes.

Q. And you inform any regulators who you believe, after analysis of the data, you believe Hiscox is obligated to inform?

A. Correct. (Bodden p.63 64)

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witness's testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

33. Kam also testified that Hiscox would want the breached data. (Kam p. 41-42)

Q. And if Hiscox data is breached within the possession of a third-party vendor in 2017, the expectation of Hiscox was that would be reported to them within a reasonable time?

A. Yes. If anything, by professional courtesy.

Q. And when that is reported then to Hiscox, what does Hiscox have to do?

A. I think it depends the nature of the data breach.

Q. Well, in this situation, it's a law firm that there's a data breach incident and it involves Hiscox litigation matters. So what does Hiscox then -- once it's reported to them that there has been such a breach, what does Hiscox expect to happen next?

A. So I can only talk about what my expectation is because, obviously, I wasn't -- if this didn't occur at the time, I would say that I would -- the questions we would ask is: what type of data; which litigation cases was involved; to what extent was it lost, so that we can understand the extent and nature of the information that is at risk, and what investigation has the law firm all planned to undergo to at least let us know what is potentially being lost or at risk.

Q. And if you requested the actual data that was believed to be in the hands of cyber criminal, would you do that?

A. What do you mean, in terms of we were in possession?

Q. Yeah. If -- if you found out there had been a data breach involving Hiscox data -

A. Yeah.

Q. -- would you want to see, if it was available, the actual data that might be in the hands of the unauthorized cyber criminals?

A. Yes.

Q. And you would want to do that to determine what your obligations were with regards to reporting to regulators and providing notice to policyholders?

A. Correct. (Kam 41-42)

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witness's testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

34. Bodden testified that as an insurance company, and subject to different regulations, Hiscox has certain legal obligations that are specific to an insurance company in the United States that may be completely different and separate from Warden Grier's obligations after a data breach. (Bodden p. 60)

Q. Because as an insurance company and subject to different regulations and all you have certain legal obligations that are specific to an insurance company operating in the United States that may be completely separate from Warden Grier's obligations after a data breach?

A. That's true, yes.

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witness's' testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

35. After learning of the hack, Hiscox CEO, Bronek Masojada formed a Hiscox Core Group that reported to Jeremy Pinchin, Hiscox Group Head of Claims. The group consisted of Ben Walter, CEO Hiscox U.S.; Kate Markham, CEO Hiscox London Market, Hannah Kam, Group Chief Risk Officer, Kylie O'Connor, Head of Communications and Tara Bodden, Senior Claims Counsel. (Depo. Ex. 23 HIC0005834) (Bodden p. 42-43)

Q. And did you become a member of what's called the Project Harry Core Group?

A. Yes.

Q. And I understand that the head of that in the United States was Ben Walter? A.That's correct.

Q. And then in the United Kingdom I think it was Kate Markham?

A. That's correct.

Q. And that the other members of the team were Hannah Kam, Kylie O'Conner and yourself?

A. Yes.

Q. And that that core group reported to Jeremy Pinchin?

A. Yes. I'm trying to think. There were a lot of people involved.

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

36. Pinchin testified Hiscox's primary focus was on informing individuals whose data had been breached.

A. The matter was quite simple. As soon as we became aware of the breach by Warden Grier - - which we had to ask them had their systems been breached - - we considered, after taking advice from external and specialist attorneys in the U.S., that there was a duty that the people whose data had been breached were informed of that fact, and we set about as speedily as possible carrying out their duty. And, therefore, our primary

focus was 100 percent ensuring that individuals whose data had been breached were informed of that fact as soon as sensible and achievable." (Pinchin p. 247-248)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

37. Pinchin testified that Hiscox hired the Cooley law firm to advise Hiscox about their legal obligations.

A. At all times we had the – who we considered to be the best attorneys in the U.S. to provide us with advice as to how to manage this matter and ensure at all times complied with the appropriate legal obligations of Hiscox towards any third party, individual or regulators and to the best of my knowledge, we always followed their advice." (Pinchin p. 103).

RESPONSE: ADMITTED for purposes of this motion.

38. Cooley had two roles – one, advise Charles River Associates (CRA) what to do with the data and two, advise Hiscox as to their notification requirements. (Walter p. 122).

Q. Right. Because Cooley -- Cooley really had two roles: One, advise CRA what to do with the data, and two, advise Hiscox as to their notification requirements?

A. That sounds right.

RESPONSE: ADMITTED for purposes of this motion

39. David Navetta was the Cooley head lawyer on this matter and he testified as to the obligations of Warden Grier and Hiscox. (Navetta page 104). (Navetta p. 23-24) (Navetta p. 115-116)

Q. Did you tell them that when they learned about it in 2018, they should tell Warden Grier it was their obligation to review the documents?

A. Warden Grier had the breach. They -- they're the only ones that have access to the documents. So yeah, it's usually the service provider's obligation to analyze their own system that they allowed hackers to get into.

Q. And did you advise Hiscox that they should tell Warden Grier that they would be responsible for reviewing the documents to determine what notification obligations Hiscox had?

A. They -- they needed to notify Hiscox of the breach. That was their obligation, including providing them enough information for Hiscox to be able do their own investigation analysis and notice. So both of those - that's basically the gist of what they should have been doing. (Navetta p. 104)

…

Q. So what specifically -- if they have an obligation to notify -- and I'm sticking with Missouri because you looked at that statute recently -- what information do they provide to Hiscox?

A. They would inform them of the incident and give them enough information to allow Hiscox, should Hiscox be considered the data owner or licensee or a -- it's a maintainer itself, to enable them to do a notice to the individuals or another party who happens to be the data owner or licensee.

Q. And do they give Hiscox that information by providing them with the Hiscox data that was compromised? (Navetta p. 23-24)

A. That's one way to do it.

Q. And is that how it was done in this particular incident?

A. I'm sorry. Can you re-ask the question? How what was --

Q. Did Warden Grier provide Hiscox the 44 gigabytes of Hiscox data that had been compromised?

A. They -- they provided access to their data, yes.

They provided a copy. (Navetta p. 23-24)

…

Q. Well, Hiscox's obligation was to notify the policyholder that potential PII had been compromised?

A. That was one of their obligations. In addition to that, providing them enough information to be able to enable them to do a notice.

Q. Right. And so you were recommending to Hiscox that they undertake that obligation; that was an obligation of their policyholder to notify individuals?

A. No. No. Hiscox, as a service provider or maintainer, has an obligation to provide notice to the data owner to enable them to be able to do their -- their duty. So it's Hiscox's obligation legally, as it was Warden Grier's.

Q. How can the --

A. It was Hiscox's obligation to provide notice independently, according to the breach laws, to its policyholders, as it was Warden Grier's should have been providing notice to Hiscox of the information that was exposed. (Navetta p. 115-116)

RESPONSE: ADMITTED for purposes of this motion.

40. Worley testified: "You look at it by the breached entity examining the information that was breached. They in most states have a duty of reasonable investigation, and they have to cooperate in order to be able to inform the data owner sufficiently so that the data owner can fulfill their responsibilities under the statute." (Worley p. 57).

Q Right. But you do that by the data owner looking at what are the potential compromised documents?

A. You look at it by the breached entity examining the information that was breached. They in most states have a duty of reasonable investigation, and they have to cooperate in order to be able to inform the data owner sufficiently so that the data owner can fulfill their responsibilities under the statutes.(Worley p. 57)

RESPONSE: ADMITTED for purposes of this motion.

41. According to Hiscox's retained expert, Worley, after Hiscox received confirmation of the hack from Warden Grier the following happened:

> "…. at Hiscox's request, Warden Grier retained Control Risks Group (CRG) to index the Compromised Server, analyze what portion of the data related to Hiscox and provide Hiscox with copies of its data on the Compromised Server. On or around April 4, 2018, Warden Grier provided Hiscox and CRG with a list of Hiscox cases that Warden Grier had handled to aid in the segregation of Hiscox's Client Data from other Warden Grier clients' data on the Compromised Server." (Worley expert report ¶ 66, 67)

RESPONSE: ADMITTED for purposes of this motion.

42. Jeremy Pinchin testified as to working with Jim Warden and cooperation.

(Pinchin page 185, 187, 181)

A. All of the efforts were focused on speed, of trying to get the data set to the experts at Charles River so they could conduct the exercise to analyze what data had been breached as effectively as possible. I worked hard and I was very appreciative of the work of Jim Warden in working with me to make sure that we did this as effectively as possible .(Pinchin p. 185

A. There's certainly -- as I've made clear throughout, our focus was the resolution of the matter and working with someone who had been a trusted adviser for us for many, many years and I expected them and I believe they did following the -- us becoming aware of the breach to work with us to resolve this matter as effectively as possible. And I believe that over those initial months, Jim Warden and I worked together collaboratively to try to make sure that we did our duties to our insureds as effectively as we could.(Pinchin p. 187)

A. I have no access to those papers to be able to articulate, other than the fact that I believe Warden Grier were concerned to make sure that we were operating together. And again, our primary focus was simply to ensure that we understood what client information had been breached, that we could understand that and we could notify our clients and our brokers and the appropriate authorities. And, therefore, at this stage we were acting totally in concert with Warden Grier to carry out that duty to our insureds as fast and as efficiently as we could.

Q. And Warden Grier was fully cooperating with that, correct?

A. At this stage, yes, they were. (Pinchin p. 181)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. Warden Grier's alleged "cooperation" after being forced to disclose the hack in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

43. Warden Grier, provided the requested Hiscox data by utilizing the services of CRG. (WGR002988) CRG praised WG for being so proactive to ensure the engagement was moving forward as quickly as possible. (WRG000917)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. Warden Grier's providing data to CRG after being forced to disclose the hack in 2018 is

immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

44. Warden Grier provided to CRG a forensic image of the compromised server that had been done by Parameter in 2017. (Warden Affidavit)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. Warden Grier's providing data to CRG after being forced to disclose the hack in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

45. Warden Grier provided a list of all policyholders of Hiscox that they had done work for over a 20 year period. (WRG002861, WRG002857 and WRG002855) (Kam p. 113)

Q. And did Warden Grier cooperate in providing details of all Hiscox claim files, policyholders, and claimants who might have been impacted?

A. I believe so, because we were able to obtain the information.(Kam p. 113)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. Warden Grier's providing a list of policyholders after being forced to disclose the hack in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

46. Hiscox requested CRG to do additional queries on the Hiscox data and WG allowed. (WGR000752-53)

RESPONSE: CONTROVERTED in that Warden Grier "allowed" CRG to do additional queries only after Hiscox demanded them and after Warden Grier had expressly instructed CRG to put the additional queries "on hold." *See* Ex. 17 (WGR000775).

47. At Hiscox's suggestion, WG utilized and paid for a ransom specialist to assist in the negotiations with the TDO. (WRG002313 and WRG002290). That specialist recommended that an additional ransom be paid if in fact the Hackers had any information that should not be made public. (Affidavit)

RESPONSE: OBJECTION pursuant to Rule 56(c)(2) that the statement "[t]hat specialist recommended that an additional ransom be paid if in fact the Hackers had any information that should not be made public" cannot be supported by admissible evidence because it is inadmissible hearsay.

Subject to that objection, ADMITTED for purposes of this motion but IMMATERIAL. That Hiscox recommended a specialist to communicate with the hackers is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

48. Warden Grier agreed to use Hiscox's PR advisers who advised WG as to the notices they should send out to clients. (WGR001001, WRG0002133, WGR000948 and WGR001174)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Hiscox recommended PR advisors after Warden Grier was forced to disclose the breach in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

49. Warden Grier agreed to enter into a Common Interest Agreement with Hiscox. Hiscox's attorney Navetta drafted the Agreement and it provided in part – "Hiscox and Warden Grier intend to take appropriate, lawful, and ethical steps to cooperate, communicate, and work jointly with respect to the Legal Matters, which is of common interest to the Parties." (Depo. Ex. 18)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That the parties entered a common interest agreement after Warden Grier was forced to disclose the breach in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

50. Warden Grier agreed to coordinate its notices to its other clients with Hiscox's notices. (WRG001026, WGR000991, WGR000449).

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Warden Grier supposedly "agreed to coordinate its notices to its other clients" after being forced to disclose the breach in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

51. Pinchin testified as to Hiscox's moral and legal obligation to notify individuals whose PII may have been compromised

> A. I think what I've made quite clear is that the moral belief in our organization was that we had to carry out what was not only the moral - - what we believed was the moral but also the legal obligation to notify

individuals, and that was first and foremost the obligation we set out to achieve.

Obviously in doing that, there would be a considerable reputational risk to our organization that third-party vendors that we had been using had been unable to keep sensitive data, PII data, safe from third-party hackers. And as a result of that, there would be damage to our brand and reputation. But, unfortunately, that's a secondary matter to the important thing, which is notifying individuals of the breach of their data. And as a result, we believe that standing up and doing the right thing, as I repeat morally and legally, was the only option that we had to do and, therefore, that's what we did and set out to do as soon as possible.

But, unfortunately, that's a secondary matter to the important thing, which is notifying individuals of the breach of the data. And as a result, we believe that standing up and doing the right thing, as I repeat morally and legally, was the only option that we had to do and therefore, that's what we did and set out to do as soon as possible." (Pinchin p. 250-251)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

52. Cooley concluded that Hiscox and Warden Grier would be considered service providers not data owners. (Depo. Ex. 41) (Depo. Ex. 207) (Navetta p. 90) (Worley p. 210-211).

Q. As to the Hiscox-related documents, was Warden Grier determined to be a service provider?

A. Yeah, Warden Grier was a service provider to Hiscox. Generally speaking, that's how we viewed them.

Q. And Hiscox was considered a service provider to their policyholders?

A. Yeah. Essentially. (Navetta p. 90)

…

Q. Right. And with regards to the Hiscox data and those individuals, Warden Grier did not have an obligation to notify those individuals?

A. I did not pull the statutes related to every individual in the data set. To answer your question, I would have had to have looked at all 50 data breach statutes and done the analysis of who's the owner, who's the service provider, is this a first-party case or a third-party case. I didn't do all that, so I just can't give you that broad of an answer.

Q. Mr. Navetta did that?

A. I think -- I think Mr. Navetta's testimony is what it is, and the analysis as he wrote it down is what he did.

Q. And he determined that both Hiscox and Warden Grier would be considered a service provider?

A. I believe that was what he decided, yes.

Q. And with that, Warden Grier didn't have the obligation to notify what they will call the Hiscox individuals?

A. I don't think Mr. Navetta, as I recall, made a determination about Warden Grier's notification responsibilities to Hiscox individuals. I believe Mr. Navetta did a legal analysis of Hiscox's obligation to notify Hiscox individuals.

Q. And his determination was there was no requirement, they simply needed to notify the policyholder?

A. That's correct. (Worley 210-211)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was merely a service provider, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

53. David Navetta, the Cooley partner, provided Hiscox with an analysis on "voluntary" notice to affected individuals by listing the Pros and Cons of this key decision point. The first pro listed was: "Will be seen as helping/ "doing the right thing." The first con listed, was: "Additional expenses." (Depo. Ex. 41, 94)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was not required to notify affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

54. Amy Yung, in-house Hiscox claims lawyer, who worked for Bodden, testified that Hiscox did not notify individuals:

Q. And at the end of the day, after this Warden Grier incident, did Hiscox notify any individuals directly?

A. No, not to my understanding

Q. Why not?

A. Following the investigation Cooley advised that Hiscox did not have any legal notification obligations to notify any individuals. (Yung depo. p. 38-39)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was not required to notify affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

55. Notes of a Harry Core team meeting for 7/20/2018 attended by Ben Walter, Steve Langan, Jeremy Pinchin, Hanna Kam, Kylie O'Connor Tony Rai , Tara Bodden and Amy Yung reflect that someone on the call said that Hiscox wanted to do what was legally required to do and not too much more. (Depo. Ex. 66) (Yung Depo. p. 154)

The document also says "legally our only obligation is to notify them that it happened. Our legal obligation ends when we've notified the customers." According to Yung: "That means that our legal obligation was to notify the customers and nothing more". (Depo. Ex. 66) (Yung Depo. p. 155)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was not required to notify affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

56. Hiscox decided that it would be up to its policyholders to notify individuals. (Bodden p. 49)

Q. So, do you recall that at the end of all the analysis of the data it was determined that Hiscox had no duty to notify any individual whose PII may have been compromised?

A. I think that's right.

Q. And that obligation, if any, to notify the individual was left up to the policyholders of Hiscox?

A. That's right (Bodden p. 49)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was not required to notify affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

57. Walter testified that Hiscox gave notice to policyholders but not individuals or regulators. (Walter p. 125-127)

Q. And do you agree that Cooley advised Hiscox that they had confirmed that Hiscox does not have any regulatory or individual notification obligations as a result of this breach?

A. Well, we -- when we found PII, we had obligations because we had to notify the people whose PII had been divulged.

Q. What I'm asking you is, is that you were informed by Cooley that they had confirmed that Hiscox does not have any regulatory or individual notification obligations as a result of this breach?

A. That sounds correct. Because there are two kinds of -- so if you think about that, there's -- we didn't have any regulatory notices. Sometimes when you have a breach, you have to tell a regulator what has happened or you have to tell the state. It depends on what state you're doing business in. And they -- I remember they confirmed that we didn't have to do that. And I remember they confirmed that we did not have any obligations to the individuals. We still needed to let our -- our policyholders know that their clients' data had been -- had been compromised because there was PII in it, but we didn't need to let the end consumer know.

Q. And did Cooley advise you as to what extent you had to tell your customer or your policyholder -- to what extent you had to tell them what PII was involved?

A. I remember that the decision -- the decision we made based on the recommendation is that we would tell the policyholders who had had -- for whom their -- their customers' PII had been divulged, that that had occurred, and that we would offer further details if they wanted them. And I remember that some did. I don't remember how many.

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed

downstream notice obligations to its policyholders even if Hiscox was not required to notify regulators or affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

58. Hiscox in-house attorney, Schonbrun, wrote: "We were managing the notification process as a courtesy to our policyholders, as we were not required to notify anyone or any regulator." (Depo. Ex. 68)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As explained in the accompanying suggestions, Cooley determined that Hiscox owed downstream notice obligations to its policyholders even if Hiscox was not required to notify affected individuals directly, and Hiscox had to do the PII analysis Warden Grier should have performed in 2017 to make that determination.

59. In fulfilling its obligation to notify policyholders, Hiscox claims to have incurred costs related to notice and a call center (Epiq - $6,189.08), public relations (Brunswick - $107,456.00), legal advice (Cooley - $276,859.50) and data analysis (Charles River Associates – $1,094,414.46). (Depo. Ex. 82)

RESPONSE: ADMITTED for purposes of this motion.

60. CRG, at the direction of Hiscox and Cooley, obtained 1,773,042 documents from Warden Grier. Cooley hired Charles River Associates (CRA) to review the 1.7 million documents for PII and confidential/sensitive information. (Depo. Ex. 206). The original proposal from CRA was for $35,012. Depo. Ex. 32)

RESPONSE: ADMITTED for purposes of this motion.

61. Hiscox made it clear that Control Risk Group (CRG) was acting for Warden Grier with respect to the data and Charles River Associates (CRA) was acting exclusively for Hiscox/Cooley. (Depo. Ex. 29). "CRA will be analyzing the data solely for us." (Depo. Ex. 28).

RESPONSE: ADMITTED for purposes of this motion that the statement accurately quotes the witnesses' testimony. CONTROVERTED inasmuch as this statement suggests or implies that Hiscox therefore suffered no damages resulting from Warden Grier's inaction. *See generally* Ex. 16 (Walter Decl.).

62. All 1,773,042 documents were provided to CRA and only 14,910 contained NPPI. (Depo. Ex. 207) (Yung p. 104)

Q. If we look at Depo. Ex. 71, that's a Harry Core Group meeting for June 20, 2018 agendA.That indicates as of that date 212 U.S. policyholders had been notified and 48 London market, right?

A. Yes.

Q. And that the PII search is complete?

A. Right.

Q. And that there are a total of 14,406 documents in scope for context review. Do you know what that means?

A. Yes. The context review was the review to determine which individuals' information belonged to which policyholder.

Q. So, you would start off, I think we saw earlier 1.7 million documents searching for PII and you ended up with 14,406 documents apparently with PII and now you're apparently trying to figure out which policyholders those apply to?

A. I believe so, yes

(Depo. Ex. 54 – Navetta – "we haven't found all that much PII. While we have PII related to 100 policyholders, there is not much there, and a lot of it is not even notifiable (e.g. a DOB)."

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That "only 14,910" of the documents contained PII is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

63. If Hiscox wanted Warden Grier to analyze the data there is usually a collaborative discussion. (Worley p. 122-123).

Q. If they had notified Hiscox within seven days of learning of the breach in February of 2017, what's your understanding as to what Hiscox's legal obligations were after they were notified?

A. It depends on what the notification said.

Q. The notification says that all of the information on our server that -- as applied to our representation of you over the last 20 years is in the hands of a cybercriminal.

A. Okay. And the question to me is?

Q. What is Hiscox's obligation then?

A So they likely would have said can you tell us what information is on the server and asked me what you -- what steps you took to mitigate the breach.

Q. Okay.

A. Asked me for the forensics. And then they would have the determination of whether they needed to notify their customers.

Q. And would they typically then negotiate with Warden Grier as to what type of analysis needed to be done on the data?

A. In my experience, there is usually a collaborative conversation about that, yes. (Worley p. 122-123)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That "there is usually a collaborative discussion" is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

64. Hiscox did not request Warden Grier to analyze the data nor did Hiscox have discussions as to who would pay for Cooley or CRA.(Pinchin p. 264-265) (Pinchin p. 192)

Q. And what discussions did you have with Jim Warden or anyone at the Warden Grier firm with regards to Hiscox's expectation, if any, that Warden Grier would pay for Charles River Associates?

A. I don't recall any specific conversations. A clear stance that we took was that Warden Grier had not made any steps within the 15-or-so month period since the hack; and, therefore, the important thing was that we move with speed to identify what PII had been breached and fulfill what we believed our moral and legal duties to inform those individuals of the breach.

Q. When you talk individuals, again, you're talking about those individuals whose PII may have been exposed to the cyber criminals?

A. I do. I confirm. (Pinchin p. 264)

…

Q. (By Mr. Horn) At any time during the period in which Charles River Associates was analyzing this data did you indicate to Warden Grier that you would expect them to pay for that?

A. I cannot recall that. I cannot recall that being the case.

Q. Charles River Associates billed on at least a monthly, maybe more -- quicker than that, but were certainly billing Hiscox on a monthly basis. Did you ever share those bills with Warden Grier?

A. As I've made clear, our focus was on ensuring that we complied with our obligations to our clients and that was our primary focus.

Q. I understand that's what you're saying your primary focus is, but my question was much simpler than that and that is as you got Charles River Associates' bills, did you ever provide those to Warden Grier?

A. We did not, I believe. (Pinchin p. 192)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Hiscox did not ask Warden Grier to analyze the data or pay for CRA or Cooley after Warden Grier was forced to disclose the breach in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

65. Pinchin did have discussions with Warden Grier as to who would be paying for CRG. (Pinchin p. 264-265)

Q. And you had had discussions apparently with Warden Grier about who would be paying for different duties that you had requested CRG to do. You had those discussions with Mr. Warden, correct?

A. Yes. They were slightly different circumstances, but you are correct, we did have those discussions.

Q. And then -- but you had no such discussions with Warden Grier with regards to who would be paying for Charles River Associates?

A. No. We believed the important thing was that the work was done as soon as possible.

Q. And, likewise, you had no discussions with Warden Grier about who would pay for the legal bills of the Cooley law firm that Hiscox hired?

A. We did not. (Pinchin p. 265)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL.

66. Pinchin cannot recall a specific discussion with Warden Grier requesting them to do an analysis of the data and find all the PII but to his understanding Warden Grier would not

have been able to carry out that themselves because he did not believe that they had "facilities and cap – and resources to undertake that themselves." (Pinchin p. 266)

> Q. And did you request Warden Grier to do some analysis of the data and they refused to do it?
>
> A. They had not done the analysis of the PII, and I believe, in correspondence, you'll see that they believed the only requirement was to provide a list of clients.
>
> Q. I understand, but my specific question is, did you have a discussion with Warden Grier and say, We want you to do an analysis of the data and find all the PII, and Warden Grier said, We will not do that?
>
> A. I cannot recall a specific conversation. We would have discussed the matter, and in my understanding, Warden Grier would not have been able to carry out that themselves.
>
> Q. And why is that?
>
> A. I don't believe that they have the facilities and cap -- and resources to undertake that themselves. (Pinchin p. 266)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Pinchin does not recall asking Warden Grier to do an analysis after Warden Grier was forced to disclose the breach in 2018 is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

67. Hiscox undertook a search of the information because it felt like it was obligated to investigate in detail what regulatory obligations applied to it and its' customers.

> Q. Does it surprise you that Hiscox, when they decided to do this million-plus-dollar analysis, didn't go to Warden Grier and say we need to figure out who's going to pay for this?
>
> A. So I understand that when Hiscox became aware of the breach in March of 2018, Jeremy Pinchin and Mr. Warden were in conversation about what the next steps would be. It is also my understanding that after the Control Risks assessment was done, Hiscox felt like it was obligated to investigate in detail what regulatory obligations applied to it and its customers, and so it undertook the search of the information then. (Worley p. 148-149)

RESPONSE: ADMITTED for purposes of this motion.

68. Warden Grier provided notice to its other clients in 2018 in conformity with the notices recommended by Sloan and Brunswick. No other client asked for a copy of its data. No other client asked Warden Grier to analyze their data. No other client has sued Warden Grier or made a claim for any costs. (Affidavit) (IGG000536, WGR002134)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Warden Grier provided notices to other clients after being forced to disclose the breach in 2018, and that those clients allegedly did not take action against Warden Grier, is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

69. Hiscox informed the New York Division of Financial Services that the incident has not materially harmed, and is not reasonably likely to materially harm, any material part of Hiscox's normal operations. (Depo. Ex. 15) (Kam page 112)

> Q. And according to paragraph 1, The incident has not materially harmed and is not reasonably likely to materially harm any material part of Hiscox's normal operations.
>
> A. Yes, I can see that wording.
>
> Q. Do you agree with that?
>
> A. After the assessment of the data that was lost, yes, I would agree.

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. That Hiscox allegedly told the DFS "that the incident has not materially harmed, and is not reasonably likely to materially harm, any material part of Hiscox's normal operations" is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

70. Hiscox is not aware that any of the breached data has been misused. (Walter p. 79)

> Q. But the harm hasn't been made public. I take it that you did have your IT people search to see if any PII had been released as of then?
>
> A. Well, we tried. We didn't know.
>
> Q. Well, you didn't find any, did you?
>
> A. We did not.

Q. In fact, you haven't found any to this day, correct?

A. We have not. Not to my knowledge, no.

Q. No customer or client has ever sued Hiscox with regards to this data breach?

A. Not that I know of, no.

Q. Or has made a claim that their PII was in any way compromised?

A. Correct.

RESPONSE: CONTROVERTED. The breached data was "misused" when it was accessed and stolen by cybercriminals, used in an extortion scheme, and then used in an attempt to re-extort Warden Grier in 2018. *See, e.g.,* Def.'s Statement of Uncontroverted Material Facts ¶¶ 3, 8, 20, 25.

71. Hiscox is not aware that any individual whose data was compromised has actually been notified. (Bodden p. 68-69, 184)

THE WITNESS: I remember concern about making sure that we provided our policyholders whose information was implicated with the information they needed so that they could comply with the law as well, so --

BY MR. HORN:

Q. And how did you make sure that your policyholders complied with the law?

A. By letting them know that information of theirs had been made available or potentially accessed.

Q. So that they then can notify individuals whose PII might have been exposed?

A. That's correct.

Q. And how did you make sure at the end of the day those individuals got notification?

A. That is generally on the policyholders' whose information were the actual data owners of that information. So, we don't -- we wouldn't follow it to the end. We have certain obligations we observed and then you give entities the information they need to be able to observe their obligation.

Q .And if the individual gets notice or not, it's then on the policyholder?

A. Depending, yes. It depends on the facts.

Q. Even though the whole purpose of this notification from the very beginning was to get information as quickly as possible to that individual so they could protect themself, to this day you have no idea if those individuals have ever even been notified?

MR. SEITZ: Objection, argumentative, asked and answered.

Go ahead.

THE WITNESS: I don't know.

BY MR. HORN:

Q. Was there any follow-up with any of your policyholders to say, we gave you a list of ten people that you should probably notify to see if they actually did it?

A. I don't know that. (Bodden p. 68-69)

…

Q. Of all the estimated number of individuals that are listed on this list, which I believe totals over eight thousand, how many of them have received notification of this breach?

MR. SEITZ: Objection, asked and answered, calls for speculation.

Go ahead.

THE WITNESS: Okay. Yeah, I think I mentioned that I don't know that.

BY MR. HORN:

Q. Do you know if any of them have?

MR. SEITZ: Same objections.

THE WITNESS: I don't know. (Bodden p. 184)

RESPONSE: ADMITTED for purposes of this motion but IMMATERIAL. As discussed in the accompanying suggestions, Hiscox's obligation was to provide downstream notice to its policyholders rather than directly to individuals. That Hiscox supposedly is not "aware" that any individual has been notified is immaterial to Hiscox's claims and does not entitle Warden Grier to judgment as a matter of law.

STATEMENT OF ADDITIONAL MATERIAL FACTS

1. Warden Grier was Hiscox's attorney when it learned of the data breach in 2017. Ex. 18 (Answer) ¶ 7; Ex. 1 (Warden Dep.) at 47:15-50:9, 56:20-58:12.

2. In late 2016 and early 2017, unauthorized individuals claiming to be The Dark Overlord accessed and exfiltrated Hiscox's client files located on one of Warden Grier's computer servers. Ex. 19 (Dep. Ex. 116); Ex. 1 (Warden Dep.) 95:6-21; Ex. 7 (Kuehn Dep.) at 31:4-32:13, 42:13-19, 47:10-48:7.

3. Among the data the hackers exfiltrated was a database Warden Grier used in connection with its work monitoring cases filed against Hiscox-insured nursing homes. The database included information about active matters, and Warden Grier was continuing to update the database through February 2017. Ex. 20 (Dep. Ex. 110); Ex. 6 (Murphy Report) ¶ 13(b) & Ex. C attached thereto; Ex. 7 (Kuehn Dep.) at 31:4-32:13, 42:13-19, 47:10-48:7.

4. As Hiscox's attorneys, Warden Grier owed Hiscox a duty of reasonable care and fiduciary duties of confidentiality and undivided loyalty in deciding how to respond to the loss of Hiscox's client information. *See* Ex. 3 (Worley Rep.) ¶¶ 84-101, *see generally* Ex. 21 (Downey Rep.); Doc. 90 at 7.

5. Hiscox submitted a 36-page expert report from Amy Reeder Worley, attached here as Exhibit 3. *See* Ex. 3 (Worley Rep.).

6. Worley is an expert data security and compliance consultant and attorney who regularly advises business, including law firms, about how to plan for, prevent, and respond to data breaches. Ex. 3 (Worley Rep.) ¶¶ 3-9.

7. Worley was deposed in this action on May 18, 2021 starting at 9:04 a.m. and continuing until 6:17 p.m. Central Time. Ex. 10 (Worley Rep.) at 5:1, 313:1.

8. Worley's report, among other things, details the standard of care for businesses (including law firms) who have suffered a data breach and how ethical obligations impact that standard when the victim is a law firm. Ex. 3 (Worley Rep.).

9. Worley opines that Warden Grier's conduct, as described in her report, fell short of Warden Grier's professional standard of care. *See generally* Ex. 3 (Worley Rep.); *see also id.* ¶ 124 ("Accordingly, for the reasons set forth in detail above, Warden Grier's response to the Data Breach fell below both the statutory and the common law standards of care applicable to (a) businesses that collect and store regulated information such as PII and PHI; and (b) attorneys that collect and store client confidential and attorney-client privileged information.").

10. Warden Grier's conduct in failing to analyze the compromised data for PII and failing to notify Hiscox about the data breach did, in fact, fall short of Warden Grier's professional standard of care. *See generally* Ex. 3 (Worley Rep.); *see also id.* ¶ 124.

11. Worley opines that Warden Grier failed to take reasonable steps to understand the nature of the impacted data, which would have revealed that the data contained PII of around 8,500 people in Hiscox's files alone. Ex. 3 (Worley Rep.) ¶¶ 103-109.

12. Warden Grier did, in fact, fail to take reasonable steps to understand the nature of the impacted data, which would have revealed that the data contained PII of around 8,500 people in Hiscox's files alone. Ex. 3 (Worley Rep.) ¶¶ 103-109.

13. Worley opines that by neglecting to analyze the data for PII Warden Grier rendered itself unable to send notifications under applicable state data breach laws, because it could not know what PII was impacted or where the affected individuals resided. Ex. 3 (Worley Rep.) ¶¶ 103-109.

14. Warden Grier did, in fact, neglect to analyze the data for PII and thereby render itself unable to send notifications under applicable state data breach laws, because it could not know what PII was impacted or where the affected individuals resided. Ex. 3 (Worley Rep.) ¶¶ 103-109.

15. Worley opines that, to meet its standard of care, Warden Grier should have analyzed the data for PII, identified the affected individuals and their states of residency, and told Hiscox about the breach and PII disclosure. Ex. 3 (Worley Rep.).

16. To meet its standard of care, Warden Grier should have analyzed the data for PII, identified the affected individuals and their states of residency, and told Hiscox about the breach and PII disclosure. Ex. 3 (Worley Rep.).

17. Worley opines that Warden Grier's standard of care is informed by, among other things, data breach reporting laws that in 2017 existed in all but three U.S. states. *See, e.g.*, Ex. 3 (Worley Rep.) ¶¶ 86-90, 98-101, 104.

18. Worley's opinion draws not just on state data breach laws but also her own experience and various articles and other sources cited in her report. *See generally* Ex. 3 (Worley Rep.).

19. Warden Grier's expert, Michael Downey, agrees that "[d]eterming a lawyer's post data breach standard of care requires, among other things, considering the applicable state or federal data breach laws that may govern the lawyer's conduct." Ex. 11 (Downey Dep.) at 12:7-14.

20. Although he opines that Warden Grier "satisfied its professional obligation" and "acted within the requisite standard of care," Downey did not disclose an opinion concerning

Warden Grier's compliance or noncompliance with applicable state or federal data breach laws. Ex. 21 (Downey Rep.).

21. Downey is not an expert in the area of state and federal data breach laws and, in his own practice, relies on experts in state data breach laws when advising law firms following a data breach. Downey does so because "I wouldn't consider myself an expert on those particular things and I would want to make sure that my law firm complied with their requirements." Ex. 11 (Downey Dep.) at 20:5-21:10.

22. Downey acknowledges that, in not reviewing the compromised data for PII, Warden Grier "may not have" complied with state data breach laws. Ex. 11 (Downey Dep.) at 67:20-68:11.

23. In his expert report, Downey relies extensively on the American Bar Association's Formal Opinion 483 to inform a lawyer's standard of care following a data breach. Ex. 11 (Downey Rep.) at 10, 17-20.

24. Formal Opinion 483 specifically references the data breach laws in the fifty states and advises attorneys to "review all potentially applicable legal response obligations" and "evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user." Ex. 11 (Downey Dep.) at 13:21-14:2, 14:25-15:18; Ex. 22 (Formal Opinion 483) at 2, 15.

25. Downey testified that, if a client sues a lawyer for advising it to fire an employee, determining the lawyer's standard of care might require expert testimony about substantive employment law. Ex. 11 (Downey Dep.) at 11:12-23.

26. Downey relies on the Rules of Professional Conduct and says those rules "serve as important guidelines for establishing and understanding the appropriate standard of care." Ex. 21 (Downey Rep.) at 10.

27. Warden Grier did not take steps to understand the nature of the impacted data, including what PII it contained and who the PII was associated with. Instead, Warden Grier decided to not look at the data but to rely on the recollections and general assumptions of its attorneys, including Warden's belief that "there might be some medical information on the server . . . other types of information like SSNs could [also] be present" but that this information was "very limited" and "at least one to two and a half years old." Ex. 1 (Warden Dep.) at 104:20-107:9.

28. Warden Grier also declined to do any searching or checking to determine whose PII might be on the affected server. Ex. 1 (Warden Dep.) at 106:22-25.

29. Warden Grier was incorrect in its belief that the PII was "very limited" or "at least one to two and half years old." In truth, the server contained PII of around 8,500 people in Hiscox's files alone. Ex. 3 (Worley Report) ¶ 80; Ex. 5 (HIC005502) at 5503. And the server included active case files, including a database Warden Grier used in its work monitoring cases filed against insured nursing homes. Ex. 6 (Murphy Report) ¶ 13(b) & Ex. C attached thereto; Ex. 7 (Kuehn Dep.) at 31:4-32:13, 42:13-19, 47:10-48:7.

30. The day it learned of the data breach, Warden Grier engaged Jim Warden and Mike Grier's former colleague, Peter Sloan ("Sloan"), whose practice involves advising clients about data breach responses. Ex. 3 (Worley Rep.) ¶ 20 (citing WGR002459).

31. On February 17, 2017, Sloan advised Warden Grier it should "consider sending two notices from the firm: one for clients and former clients of the firm whose confidential file materials you believe were compromised in the hack, and a second for individuals whose PII you

believe was compromised (such as name in combination with SSN/financial account/governmental ID number, etc.)." Ex. 23 (Dep. Ex. 111) at 534.

32. Sloan said "the client notice is driven by the implications of the pertinent professional rules of conduct, and the individual notice is driven by compliance with applicable state statutes for data breach notification." Ex. 23 (Dep. Ex. 111) at 534.

33. Sloan told Warden Grier it had to understand the data on the compromised server to comply with relevant state data breach laws. Specifically, Sloan said:

> Virtually every state has a PII breach notification statute defining what is PII, requiring notice in prescribed circumstances, and often mandating the form of notice. As mentioned, these statutes apply based upon the residency of the affected individuals, so one normally (1) *determines which individuals' PII was compromised*, (2) *confirms their residency*, and then (3) *reviews the requirements based upon the applicable states' laws*.

Ex. 24 (Dep. Ex. 112) at 523.

34. Sloan prepared notices for clients and affected individuals, which Warden Grier did not send. Ex. 23 (Dep. Ex. 111); Ex. 24 (Dep. Ex. 112).

35. The contract Warden Grier entered with hackers claiming to be The Dark Overlord was signed with Adolf Hitler's signature (for the hackers) and the phrase "Stella is a dog" (for Warden Grier). Ex. 25 (Grier Dep.) at 119:24-120:9, 124:4-125:17.

36. Concerning the ransom, Worley testified that Warden Grier could have paid the ransom but then performed the PII analysis and notifications anyway. Among other things, Worley testified "[g]enerally, in cases like this, where we know there's been exfiltration, you pay the ransom to buy time, to try to protect the data while you are doing the other analysis, which is figuring out what data was impacted and what regulations apply." Ex. 10 (Worley Dep.) at 77:1-81:2; *see also id.* at 76:12-80:14; Ex. 1 (Warden Dep.) at 133:17-134:8; Ex. 11 (Downey Dep.) at 45:3-50:15.

37. Worley testified that, when data is exfiltrated, breach notifications are necessary even after paying a ransom because "[y[ou know, once you have the Social Security number and date of birth, identity theft becomes very easy, and so we're not worried as much about the bad guy publishing the information as the harm in fact, that the bad guys now have copies of the information and they can continue to perpetrate further crimes with it." Ex. 10 (Worley Dep.) at 77:23-78:21.

38. Warden Grier's memorandum documenting its decision not to notify clients or affected individuals expressly contemplated that the hackers might not delete the data, even after Warden Grier paid a ransom. Ex. 26 (Dep. Ex. 116) at 4 ("An additional scenario seems possible – that we pay TDO's demands and it then does not adhere to its vows.").

39. Warden Grier's memorandum says "the most likely way that TDO would break its vows would be to come back to us for more money." Ex. 26 (Dep. Ex. 116) at 4.

40. Warden Grier's memorandum says "we conclude that TDO would come back to us for more money before releasing or publicizing the information, giving us an opportunity to reject the renewed demand and, if it becomes reasonably likely that TDO has released or imminently will release or publish, to take steps to notify clients and others potentially affected." Ex. 26 (Dep. Ex. 116) at 4.

41. Warden Grier's memorandum says Warden Grier would "notify our clients and others only if we learn that TDO is violating its vows." Ex. 26 (Dep. Ex. 116) at 4.

42. When the hackers violated their vows by resurfacing and demanding more money in 2018, Warden Grier still did not notify Hiscox about the data breach until Hiscox confronted Warden Grier, even after Sloan advised Warden Grier to "call Hiscox and give them the narrative." Ex. 1 (Warden Dep.) at 158:4-160:11.

43. In April 2017, Warden Grier attorneys wrote that "[w]e might have wasted $60k [the ransom] as it appears to me we are headed back toward [client] disclosure" Ex. 8 (Dep. Ex. 133).

44. In April 2018, Mike Grier sent his colleagues the following message:

> The estimate does not include travel expenses. So this is at least $18,000 plus the $10k for Peter last week - and we are just getting started. Think about shutting down - starting a new entity in Kansas- leave $200k in WG to clean up this mess, file notice of dissolution. This way we have chance to keep value of future work and distance ourselves from a bottomless pit of expense. I assume, as with rest of the world, Hiscox thinks we are rich - and CRG will be surprised that we are only a 3.5 lawyer firm - my two cents but at $20k a week in costs we will arrive at bottom of bucket real quick. Please take my comments as dead serious

Ex. 9 (Dep. Ex. 120).

45. Concerning downstream notice, Worley testified as follows.

> Q. And you know that, in this particular case, Cooley advised Hiscox that they had no individual notification requirements?
>
> A. I understand that that is what Cooley explained to Hiscox, and I understand that Hiscox then notified its customers and provided them with the names or the information about the individuals so that its customers could comply with their reporting obligations, which is how it works.
>
> . . . . .
>
> Q. Did Hiscox do anything to make sure that that was done?
>
> A. I don't know.
>
> Q. Okay. Wouldn't you expect them to do that?
>
> A. Not necessarily.
>
> Q. Why not necessarily?
>
> A. It depends on the statute. So we expect the organization to do what's required. If the requirement is to notify the data owner, that's what you do. And there's a good reason for that. The reason is it needs to be clear who's doing the notifying because we don't want to confuse the consumer. We don't want them to think, for example, that there's two breaches, that they're getting a call from Hiscox and they're getting a call from ABC insured.

> So the reason the law delineates, you know, service providers notify the owner is to protect the consumer so they're getting -- we know who's the person who's notifying. What Hiscox did have to do, and I understand that they did, is provide their downstream customers with the information about the individuals and the compromised data elements so that the insureds, the customers, were able to meet their notification obligations.
>
> Q. Okay. And as I understand it, you believe that Warden Grier should have given that information first to Hiscox, and then Hiscox would make a decision to give it to their policyholders, and then the policyholder would make the decision as to whether to notify the individual?
>
> A. The notification obligations turn on the data and the state law or federal law implicated. Generally the way it works is service provider provides -- the upstream service provider provides to data owner. It works that way almost everywhere in the world.
>
> Now, there are times when an entity is both things, so you could have information that came to you as a data owner and also came to you as a service provider. And those have to be looked at specifically to determine, you know, what are your obligations for that person for those data elements in that circumstance under law.

Ex. 10 (Worley Dep.) at 137:14-22, 138:5-140:6

46. Hiscox incurred around $1.5 million in damages because it paid vendors to oversee and perform the PII analysis and notification process that Warden Grier should have done when it learned of the hack in 2017. *See* Ex. 16 (Walter Decl.) & Exhibit A attached thereto.

47. Hiscox would not have incurred those expenses if Warden Grier had met its standard of care and fiduciary duties. *See* Ex. 16 (Walter Decl.) & Exhibit A attached thereto; Ex. 3 (Worley Rep.).

48. Although, after reviewing the PII, Cooley advised Hiscox it did not have send breach notifications to individuals, Cooley did advise Hiscox of its obligation to notify certain policyholders about the unauthorized disclosure of PII. *See, e.g.*, Ex. 27 (Dep. Ex. 94) at 4152 ("Based on what we are seeing, it appears likely that Hiscox's primary legal obligation will be to notify the 'data owner' of the incident (or potentially a downstream service provider), and not the affected individuals directly."); Ex. 5 (HIC05502) at 5503 (detailing "Hiscox's Mandatory

Notices" including that "Hiscox must provide email or written notice to customers with details about the incident and affected individuals. Must be sufficient to allow the customers to make their own determinations about breach notification obligations and to provide notice directly to individual.").

49. Worley opines that Warden Grier's ethical obligations, as informed by the Model Rules of Professional Conduct, required them to notify Hiscox about the data breach. Ex. 3 (Worley Rep.) ¶¶ 91-95.

ARGUMENT

I. Introduction

After learning in February 2017 that cybercriminals exfiltrated more than a terabyte of its client files, Warden Grier ignored its obligations under the Rules of Professional Conduct, state data breach laws in multiple states, and the advice of its own attorney in deciding not to tell clients about the data breach or even review the compromised data for personally identifiable information ("PII"), like health information or social security numbers. When Warden Grier's longtime client Hiscox learned about the data breach in March 2018 (not from its attorneys but from the hackers themselves), it had to do what Warden Grier should have done in the first place: analyze the data for PII and send data breach notifications. Hiscox now seeks to recover the costs of those efforts as damages, because they would have been unnecessary had Warden Grier complied with its standard of care and fiduciary duties when it learned of the hack in 2017.

In the current motion, Warden Grier asks the Court for summary judgment because, among other things, Warden Grier "was not negligent"[1] and Hiscox supposedly has no damages. The Court should deny the motion for five reasons.

First, Warden Grier does not dispute it owed Hiscox duties as Hiscox's attorneys. Nor could it. In cases, like this one, between clients and their attorneys, the concept of duty is supplied by the defendant's profession itself. As Hiscox's attorneys, Warden Grier owed Hiscox a duty of care (that is, to comply with professional standards) and fiduciary duties of confidentiality and undivided loyalty. The dispute is not whether Warden Grier owed Hiscox duties (it did) but whether Warden Grier met the standard of care arising from those duties after learning of the hack in 2017.

[1] Doc. 90, at 4.

Second, whether Warden Grier met its standard of care is a fact issue that implicates state data breach laws. Hiscox provided expert testimony from a data security compliance consultant and attorney explaining that Warden Grier's standard of care is informed by, among other things, state data breach laws and that Warden Grier fell short of that standard when it failed to do the PII analysis and notifications those laws require. For its part, Warden Grier's expert says the law firm met its standard of care. But Warden Grier's expert also acknowledges that determining the standard of care "requires, among other things, *considering the applicable state or federal data breach laws*," and that Warden Grier's conduct "may not have" complied with those laws. Statement of Add'l Material Facts ("AMF") ¶¶ 19, 22. Given the dueling expert reports and agreement that state data breach laws inform the standard of care (as well as ample evidence of negligence from Warden Grier's own documents), the Court should reject Warden Grier's motion.

Third, whether Warden Grier violated its duty of loyalty is also a fact dispute. There is evidence from which a jury can infer that Warden Grier put its own interests above the interests of its clients when it decided not to review the data for PII or tell clients about the breach. This evidence includes, among other things, Warden Grier ignoring its attorney's advice about its ethical obligations and Warden Grier's internal messages about how the lawyers could evade their responsibilities and "distance ourselves from a bottomless pit of expense." AMF ¶¶ 27-28, 30-34.

Fourth, whether Hiscox suffered damages from Warden Grier's inaction is another fact dispute. The parties genuinely dispute whether Hiscox would have incurred costs for the PII review and notification process if Warden Grier had met its duty of care and fiduciary obligations in 2017.

Fifth, Warden Grier's arguments about indemnification are beside the point. Hiscox did not plead a claim for indemnification and will not pursue one at trial.

The Court should deny summary judgment and re-set this matter for trial.

II. Genuine issues of material facts preclude summary judgment on Hiscox's professional negligence and fiduciary duty claims.

"A moving party is entitled to summary judgment on a claim only upon a showing that 'there is no genuine issue of material fact and that the moving party is entitled to a judgment as a matter of law.'" *Spencer v. Barton Cty. Ambulance Dist.*, No. 16-05-083-CV-SW-RK, 2017 WL 7038130, at *1 (W.D. Mo. Sept. 13, 2017) (quoting *Williams v. City of St. Louis*, 783 F.2d 114, 115 (8th Cir. 1986). "In applying this standard, the Court must view the evidence in the light most favorable to the non-moving party, giving that party the benefit of all inferences that may be reasonably drawn from the evidence." *Id.* (citing *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587-88 (1986) and *Tyler v. Harper*, 744 F.2d 653, 655 (8th Cir. 1984)). The burden is on the moving party to establish both the lack of a genuine issue of material fact and that the party is entitled to judgment as a matter of law. *See* Fed. R. Civ. P. 56(c); *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 586-87 (1986).

Here there are genuine issues of material fact precluding summary judgment on Hiscox's professional negligence and fiduciary duty claims. And none of Warden Grier's arguments entitle it to judgment as a matter of law either. As explained more below, there are genuine disputes over whether Warden Grier met its standard of care and the fiduciary duties applying to attorneys, and over causation and damages. The Court should deny summary judgment accordingly.

A. As Hiscox's attorneys, Warden Grier owed Hiscox a duty of care and fiduciary duties of confidentiality and undivided loyalty

Warden Grier is right that typically the "question of whether a legal duty exists . . . is a question of law to be decided by the court." Doc. 90 at 10. But there is no question about whether legal duties exist here. They do exist because Warden Grier was Hiscox's attorney.

Under Missouri law, attorneys owe their clients a "duty to exercise due care" and "basic fiduciary obligations of undivided loyalty and confidentiality." *Klemme v. Best*, 941 S.W.2d 493,

495 (Mo. banc 1997). These duties come from the attorney-client relationship itself. *See, e.g.*, *Meyer v. Carson and Coil*, 614 S.W.3d 618, 625 (Mo. App. 2020). So the existence of duty is generally not at issue in cases against attorneys, unless the plaintiff is someone other than the client. *Id.*; *accord Ostrander v. O'Banion*, 152 S.W. 3d 333, 338 & n.2 (Mo. App. 2004) ("In this medical negligence case, as in many other negligence cases, there is no question of legal duty" because "[a] legal duty is created by the existence of a physician-patient relationship").[2]

In fact, "duty" is not even an element of a professional negligence claim against an attorney. The elements instead are (1) an attorney-client relationship; (2) negligence (3) proximate causation, and (4) damages. *Klemme v. Best*, 941 S.W.2d at 495. As the Missouri Court of Appeals explained, plaintiffs must establish "an attorney-client relationship" instead of duty because "from that relationship arises the duty to exercise reasonable care in the attorney's practice of the profession." *Meyer*, 614 S.W.3d at 625.

Here the parties had an attorney-client relationship when Warden Grier learned of the data breach in 2017. AMF ¶ 1. That breach led to the exfiltration of Hiscox's client files, including a database Warden Grier used to monitor active cases. *Id*. ¶¶ 2-3. Because Warden Grier was Hiscox's attorney, it owed Hiscox a duty of reasonable care and fiduciary duties of confidentiality and loyalty in deciding how to respond to the loss of that information. Doc. 90 at 7; AMF ¶ 4. There is no dispute over the attorney-client relationship or that there was a "duty" here.

B. Whether Warden Grier met the standard of care for attorneys is a fact dispute.

Unlike duty, whether a lawyer was negligent "is a question of fact, not a question of law." *Zweifel v. Zenge and Smith*, 778 S.W.2d 372, 373 (Mo. App. 1989). Except in unusual cases,

[2] The Eighth Circuit cited *Ostrander's* discussion of duty approvingly in *Rosemann v. Sigillito*, 785 F.3d 1175, 1179-80 (8th Cir. 2015), a legal malpractice case.

parties use expert witnesses "to tell the jury what the defendant should or should not have done under the particular circumstances of the case and whether the doing of the act or the failure to do that act violated the standards of care of the profession." *Rosemann*, 785 F.3d at 1179-80 (citing *Ostrander*, 152 S.W.3d at 338). It is then up to the jury to resolve conflicts in expert testimony while "the trial judge sets aside his [or her] own expertise and becomes a layman." *Roberts v. Sokol*, 330 S.W.3d 576, 581 (Mo. App. 2011). The question of a lawyer's negligence is a matter of law only "if reasonable men (not reasonable *lawyers*) would have no grounds in the evidence to disagree." *Id*. (emphasis in original).

Here Hiscox has expert testimony from a data security compliance attorney, Amy Reeder Worley, in both a 36-page report (AMF ¶¶ 5-6) and during nine hours of deposition (*id*. ¶ 7). Worley is an attorney who leads a global privacy and data security consulting practice, where she advises businesses and law firms how to respond to data breaches. *Id*. ¶ 6. Worley details the standard of care for businesses (including law firms) who have suffered a data breach and how ethical obligations impact that standard when the victim is a law firm. *Id*. ¶ 8.

Worley ultimately concludes, among other things, that Warden Grier's conduct fell short of its professional standard of care. AMF ¶¶ 9-10. Worley says Warden Grier failed to take reasonable steps to understand the nature of the impacted data, which would have revealed that it contained PII of around 8,500 people in Hiscox's files alone. *Id*. ¶¶ 11-12. And Worley opines that by neglecting to analyze the data for PII Warden Grier rendered itself unable to send notifications under applicable state data breach laws, because it could not know what PII was impacted or where the affected individuals resided. *Id*. ¶¶ 13-14. If Warden Grier had done things correctly, it would have analyzed the data for PII, identified the affected individuals and their states of residency, and

told Hiscox about the breach and PII disclosure. *Id*. ¶¶ 15-16. Worley's testimony is alone sufficient to create a genuine dispute about Warden Grier's negligence.

1. Determining a lawyer's post data breach standard of care requires considering state data breach laws, as Warden Grier's expert admits.

In its motion, Warden Grier argues Missouri's data breach statute "does not allow for a private cause of action" and that Hiscox is supposedly trying to "bring claims under the entire statutory scheme of data breach statutes across the United States." Doc. 90, at 12. Warden Grier also argues Worley's reliance on state data breach laws amounts to "negligence *per se*," which Warden Grier says applies only in personal injury or property damage cases. *Id*. at 11 n.6.

At their core, these arguments misunderstand how plaintiffs prove professional negligence cases. Standard-of-care experts in legal malpractice cases testify about legal rules and statutes all the time. They do so because they have to tell the jury "what an attorney, under the same or similar circumstances, would have done and why [the defendant's] actions were unacceptable." *Rosemann*, 785 F.3d at 1180 (citing *Roberts*, 330 S.W.3d at 580) (cleaned up). If a client sues a lawyer for advising it to fire an employee, for example, determining the lawyer's standard of care requires expert testimony about substantive employment law, so the jury knows what the attorney did wrong or should have done differently. AMF ¶ 25. So too here. The point of Worley's testimony about state data breach laws is not to enforce those laws against Warden Grier or invoke negligence per se, it's that the data breach laws are relevant to the *standard of care* for a law firm that suffers a data breach. *Id*. ¶¶ 17-18.

Indeed, entering summary judgment here because Hiscox's expert relies on state data breach laws would be particularly inappropriate because ***Warden Grier's own expert*** testified those laws are relevant to the standard of care. Warden Grier's standard-of-care expert, Michael Downey, testified that "[d]eterming a lawyer's post data breach standard of care requires, among

other things, considering the applicable state or federal data breach laws that may govern the lawyer's conduct." AMF ¶ 19. Downey also relied extensively on the ABA's Formal Opinion 483 to inform a lawyer's standard of care following a data breach. *Id*. ¶ 23. And that Opinion specifically references the data breach laws in the fifty states and advises attorneys to "review all potentially applicable legal response obligations" and "evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user." *Id*. ¶ 24. Warden Grier cannot contend Hiscox should lose the case just because its expert testified about something everyone, including Warden Grier's expert, agrees is relevant to the standard of care.

Nor is it significant to say Missouri's data breach statute lacks a private right of action. Doc. 90 at 11. The Rules of Professional Conduct also lack a private right of action. *See generally* Mo. Sup. Ct. R., rule 4; *see also Greening v. Klamen*, 652 S.W.2d 730, 734 (Mo. App. 1983). Yet courts permit testimony about the Rules of Professional Conduct to inform an attorney's standard of care. *See* Restatement (Third) of the Law Governing Lawyers §52(2)(c) & cmt. f. Indeed, Warden Grier itself relies on the Rules of Professional Conduct to explain what it should have done in this case—in both its brief and expert report. *See* Doc. 90 at 8; AMF ¶ 26 (the rules "serve as important guidelines for establishing and understanding the appropriate standard of care").

In yet another example, HIPAA lacks a private right of action too. But in negligence cases arising from data disclosures courts allow HIPAA's Privacy Rule to "inform the relevant standard of care." *Byrne v. Avery Ctr. for Obstetrics and Gynecology, P.C.*, 102 A.3d 32, 46-48 (Conn. 2014) (surveying state and federal cases). That some or all state data breach laws lack a private right of action does not mean Hiscox is prohibited from using expert testimony about those laws as evidence of Warden Grier's standard of care.

Finally, although Worley opined in depth about what Warden Grier should have done to comply with state data breach laws, her report is not limited solely to those issues. Worley has real-world experience advising business, including law firms, following a data breach. AMF ¶¶ 6, 18 . Her report draws not just from the state data breach laws but also her own experience and a litany of articles and other sources, including the special obligations arising from the attorney-client relationship and the same ABA opinions Downey discusses. *Id*. ¶ 18. That Worley also draws on her experience with compliance under state data breach laws—a critical component of the standard of care—does not entitle Warden Grier to summary judgment.

2. A jury could reasonably infer that Warden Grier failed to meet its standard of care, by not analyzing the data for PII or notifying Hiscox about the breach, and that Warden Grier was therefore negligent.

Warden Grier also argues it acted "reasonabl[y]" and was "not negligent" in its response to the data breach. Doc. 90 at 8, 10. In doing so, Warden Grier focuses mostly on its decision to pay ransom and how that decision supposedly kept client information confidential. *Id*. at 8-10. Again, whether Warden Grier was negligent is a fact issue for the jury, unless there is no evidence for the jury to find otherwise. There is ample evidence of Warden Grier's negligence here.

First, as noted above, Worley testified that Warden Grier should have taken steps to understand the nature of the impacted data, including what PII it contained and who the PII was associated with. AMF ¶¶ 10-16. Rather than take those steps, Warden Grier decided to not even look at the data but to rely on their recollections and general assumptions, including Warden's belief that "there might be some medical information on the server . . . other types of information like SSNs could [also] be present" but that this information was "very limited" and "at least one to two and a half years old." *Id*. ¶¶ 27-28. This belief proved wrong. The server contained PII for 8,500 people in Hiscox's files alone, including from active case files. *Id*. ¶ 29.

Second, Warden Grier ignored its *own attorney's advice* when it decided not to review the data for PII or send breach notifications. The same day Warden Grier learned about the hack, it hired Peter Sloan, a former colleague of Mike Grier and Jim Warden's, who advises clients about data breach responses. AMF ¶ 30. Sloan told Warden Grier to "consider sending two notices from the firm: one for clients and former clients of the firm whose confidential file materials you believe were compromised in the hack, and a second for individuals whose PII you believe was compromised (such as name in combination with SSN/financial account/governmental ID number, etc.)." *Id*. ¶ 31. According to Sloan, "the client notice is driven by the implications of the pertinent professional rules of conduct, and the individual notice is driven by compliance with applicable state statutes for data breach notification." *Id*. ¶ 32.

Like Worley, Sloan also told Warden Grier they had to understand the data on the compromised server to comply with relevant state data breach laws. Sloan said:

> Virtually every state has a PII breach notification statute defining what is PII, requiring notice in prescribed circumstances, and often mandating the form of notice. As mentioned, these statutes apply based upon the residency of the affected individuals, so one normally (1) *determines which individuals' PII was compromised*, (2) *confirms their residency*, and then (3) *reviews the requirements based upon the applicable states' laws*.

AMF ¶ 33 (emphasis added). Sloan even prepared notices for clients and affected individuals. *Id*. ¶ 34. Warden Grier then decided not to follow Sloan's advice to determine whose PII was compromised, confirm the individuals' states of residency, or send notifications. *Id*. ¶ 27-28.

Third, Warden Grier focuses mostly on the ransom and says paying it was "reasonable." Doc. 90 at 8. But the claim here turns on the failure to evaluate the data for PII and notify Hiscox, not Warden Grier's decision to pay ransom. In any event, the evidence will show that in paying ransom Warden Grier signed a "contract" in which the hackers promised to delete the data, but that this contract was signed with Adolf Hitler's signature (for the hackers) and the phrase "Stella

is a dog" (for Warden Grier). AMF ¶ 35. Whether Warden Grier acted reasonably in trusting a sham contract with cybercriminals posing as Adolf Hitler is a fact issue for the jury to decide.

Even more to the point, Warden Grier's arguments about paying ransom fall apart if you consider the firm could have paid ransom but then performed the PII analysis and notifications *anyway*. That is precisely what Worley said Warden Grier could have done to comply with its standard of care: "[i]n cases like this, where we know there's been exfiltration, you pay the ransom to buy time, to try to protect the data while you are doing the other analysis, which is figuring out what data was impacted and what regulations apply." AMF ¶ 36-37. So Warden Grier still should have reviewed the data for PII and sent notifications, not only because data breach laws require it, but also because criminals sell PII on secondary markets, for use in identify theft. *Id*. ¶ 37.

Fourth, Warden Grier's self-serving memorandum about its decision not to send data breach notifications expressly contemplated that the hackers might not delete the data. AMF ¶ 38. Warden Grier reasoned that, if the hackers broke their promise, they would come back to Warden Grier for more money. AMF ¶ 39. If the hackers resurfaced, Warden Grier said they would notify clients before the hackers took reprisals. *Id*. ¶ 40-41.

As it happens, the hackers *did* resurface demanding more money and claiming not to have destroyed the data. SUMF ¶ 25. Ignoring their memo, Warden Grier *again* decided not to tell clients, even after Sloan urged them to "call Hiscox and give them the narrative" AMF ¶ 42.

Fifth, Warden Grier does not even rebut Worley's testimony that its conduct fell below the standard of care. Downey says Warden Grier "satisfied its professional obligation" and "acted within the requisite standard of care." AMF ¶ 20. But Downey does not opine on state data breach laws, even though he agrees they are relevant to the standard of care, and even though he acknowledges Warden Grier may not have complied with them. *Id*. ¶¶ 19-22. Even more, Downey

testified that, in his own practice, he relies on experts in state data breach laws when advising law firms following a data breach. *Id*. ¶ 21. He does so because "I wouldn't consider myself an expert on those particular things and I would want to make sure that my law firm complied with their requirements." *Id*. Downey cannot rebut Worley's testimony here because she testifies about issues he acknowledges are relevant to the standard of care but outside his area of expertise.

Warden Grier also cites Sloan's testimony that its decision was "appropriate" but this also cannot rebut Worley. Doc. 90 at 9. As discussed in Hiscox's motion to strike, Sloan cannot opine on Warden Grier's compliance with the standard of care because he did not disclose this opinion.

Sixth, the information presented here is only a snapshot of what Hiscox will present at trial. Warden Grier's internal messages show a single-minded focus not on fulfilling their obligations to clients but on saving money. They wrote, for example, about having "wasted [the] $60k" ransom if they had to make client disclosures. AMF ¶ 43. And, when they got a $18,000 bill from the incident, Grier urged his colleagues to shut down the firm and move to Kansas:

> last week - and we are just getting started. Think about shutting down - starting a new entity in Kansas- leave $200k in WG to clean up this mess, file notice of dissolution. This way we have chance to keep value of future work and distance ourselves from a bottomless pit of expense. I assume, as with rest of the world, Hiscox thinks we are rich - and CRG will be surprised that we are only a 3.5 lawyer firm - my two cents but at $20k a week in costs we will arrive at bottom of bucket real quick. Please take my comments as dead serious

Id. ¶ 44 (emphasis added).

In summary, Hiscox has sufficient evidence, in the form of expert opinion testimony and from Warden Grier's own documents, that Warden Grier's conduct fell below the professional standard of care applying to attorneys. A jury could find that Warden Grier committed professional negligence, especially if all inferences are in Hiscox's favor, as they are for this motion. Summary judgment is improper.

3. That Hiscox lacks PII and is not a "consumer" makes no difference.

Warden Grier also argues it cannot be liable for negligence because Hiscox lacks PII of its own and is not a "consumer" under Missouri's data breach statute. Doc. 90 at 6, 11-12. Those arguments misconstrue Hiscox's standard-of-care evidence.

First, it is true Hiscox has no PII of its own. Corporate entities like Hiscox don't have "personally" identifiable information. But merely stating that as fact does not mean Hiscox cannot hold Warden Grier liable for its negligence.

Along with the duties Warden Grier owed Hiscox as its attorneys, Worley testified that entities, like law firms, also have obligations under state data breach laws to analyze data for PII so they can notify *other entities* about a data breach. AMF ¶ 45. This happens because corporate entities (especially insurers like Hiscox) possess sensitive PII belonging to individuals, either because the entities collect the information from insureds or because they receive an individual's PII from another company. *Id*. Compliance with data breach laws requires the breached party to review the data for PII not just to determine obligations to individuals but also to send notice "downstream" to the data owner or service provider from whom the data originated. *Id*.; *see also* AMF ¶ 48. So Warden Grier is wrong to suggest it owed no duties to review PII or notify Hiscox or that it cannot be negligent just because Hiscox lacks PII of its own.

Second, Warden Grier is also wrong that Missouri law requires notice only "to affected consumers" Doc. 90 at 11 (citing RSMo § 407.1500.2(6)) (emphasis in original). When data about Missouri residents originates from another business entity, a breached party sometimes must notify "the owner or licensee of the information" even if that party is an out-of-state business entity. RSMo § 407.1500.2(2). This rule tracks the downstream notice Worley explained at deposition and that Cooley told Hiscox it as obliged to do. AMF ¶ 48. Warden Grier's arguments about lack

of corporate PII and notice requirements for affected consumers do not excuse Warden Grier from complying with its standard of care as to Hiscox.

C. Whether Warden Grier violated its duty of loyalty is a fact dispute.

Like negligence, Hiscox also disputes whether Warden Grier breached its fiduciary duties. As summarized above, a jury could find Warden Grier put its interests above its clients, by ignoring its attorney's ethics advice and seeking to evade its client responsibilities. AMF ¶¶ 27-34, 43-44.

In its motion, Warden Grier makes two arguments that supposedly entitle it to judgment on the fiduciary duty claim, each of which fails.

First, Warden Grier quotes Hiscox's June 2020 opposition to a motion to dismiss, in which Hiscox said its claims "arise from the more mundane area of [Warden Grier's] data security practices" instead of Warden Grier's legal services Doc. 90 at 6. Since it is only a data storage provider, says Warden Grier, "there is no fiduciary relationship." *Id*. at 7.

This argument misconstrues the record. When it opposed the motion to dismiss, Hiscox had no discovery and pleaded claims based on Warden Grier's inadequate data security. *See* Doc. 16. The point Hiscox made in opposition was that this theory (the fact of the hack) did not necessarily arise from Warden Grier's provision of legal services. *Id*. The Court agreed and allowed Hiscox to pursue alternative theories. Doc. 37. But it is incorrect to say Hiscox's fiduciary duty claim now arises out of something other than the attorney-client relationship.[3]

Second, Warden Grier next argues the fiduciary duty claim fails because the Rules of Professional Conduct do not expressly require notification and Warden Grier was supposedly

[3] Warden Grier did not brief the fifth element of a fiduciary duty claim in its summary judgment papers—that "no other recognized tort encompasses the facts alleged." *Klemme*, 941 S.W.2d at 496. Although Warden Grier reserves the right to proceed on alternative theories (particularly if the court finds the legal malpractice claim legally defective), Warden Grier expects the Court will ultimately instruct the jury on professional negligence.

acting in its clients' best interests. Doc. 90 at 8-9. This too is genuinely disputed. Worley opines, for example, that the Rules do require notification. AMF ¶ 49. And Downey relies on an ABA Opinion interpreting Model Rule 1.4 that unequivocally says "[w]hen a data breach occurs involving . . . material client confidential information a lawyer has a duty to notify the client of the breach." AMF ¶¶ 23-24. In any event, Warden Grier's arguments about acting in the best interest of clients is just their spin on the evidence; a jury could find the opposite.

D. Whether Warden Grier's conduct caused damage to Hiscox is a fact dispute.

Warden Grier also seeks summary judgment because Hiscox supposedly lacks damages from the data breach. In a professional negligence case, the jury decides whether the attorney was negligent and, if so, whether "such negligence directly caused or directly contributed to cause[4] damage to plaintiff." *SKMDV Holdings, Inc. v. Green Jacobson, P.C.*, 494 S.W.3d 537, 554 (Mo. App. 2016). Again, whether Warden Grier's negligence caused Hiscox damage is disputed.

Here Hiscox incurred around $1.5 million in damages because it paid vendors to oversee and perform the PII analysis and notification process that Warden Grier should have done when it learned of the hack in 2017. AMF ¶ 46. The jury can infer that Warden Grier's negligence and breach of fiduciary duty directly caused those damages because Hiscox would not have incurred them if Warden Grier had met its standard of care or fiduciary duties. *Id*. ¶ 47.

Warden Grier has three arguments in response, none of which withstand scrutiny.

First, that Hiscox told a regulator in 2019 that the data breach "is not reasonably likely to materially harm, any material part of Hiscox's normal operations" is not "fatal." Doc. 90 at 13. Hiscox is an international insurance company. It is no doubt true that paying $1.5 million because of Warden Grier's failings made no difference to "any material part of Hiscox's normal operations"

[4] The "contributed to" language is available here. *See SKM Holdings, Inc.*, 494 S.W.3d at 554-55.

or to Hiscox's brand or reputation. But saying Hiscox suffered no business disruptions or reputational harm is different than saying Hiscox suffered no damage. Hiscox is aware of no rule saying it can only recover "material" damages or damages affecting its "normal operations."

Second, Warden Grier's argument that Hiscox "would have undertaken the same analysis of the Hiscox-related data in 2017" misconstrues the testimony. The witnesses did not say Hiscox would have taken the same actions in 2017. They said Hiscox would have taken the same actions in 2017 *if Warden Grier had refused its obligations to analyze data for PII or send breach notifications*. SUMF ¶ 30. In other words, it was Warden Grier's breach of the standard of care that caused Hiscox's damages, not the "delay" in finding out about the hack. Doc. 90 at 6.

Third, Warden Grier argues intermittently that Hiscox's expense was "extraneous" and "voluntary." Doc. 90 at 18. If this is an argument about causation and damages, it is genuinely disputed. True, Hiscox ultimately determined it did not have to notify affected individuals. But the PII review process necessary to make that determination was not "voluntary" and Hiscox was still *required* to send downstream notifications to its corporate policyholders. AMF ¶ 48. Hiscox would not have incurred these mandatory expenses if Warden Grier had met its standard of care and fiduciary obligations to do the PII analysis that Hiscox later performed. *Id*. ¶¶ 46-47.

III. Hiscox made no indemnification claim so Warden Grier's arguments about indemnification are irrelevant.

Finally, Warden Grier's arguments about common law indemnification are a non sequitur. Hiscox has not raised an indemnification claim and will not pursue one at trial.

CONCLUSION

For all these reasons, Hiscox asks the Court to deny Warden Grier's motion for summary judgment and re-set this matter for trial.

DATED: October 6, 2021

Respectfully submitted,

Spencer Fane LLP

By */s/Michael W. Seitz*

Daniel E. Blegen, MO #47276
Michael W. Seitz MO #69337
1000 Walnut, Suite 1400
Kansas City, MO 64106
(816) 292-8823
(816) 474-3216 (fax)
dblegen@spencerfane.com
mseitz@spencerfane.com
Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

On October 6, 2021, a copy of this document was filed using the Court's electronic CM/ECF case filing system, which provides service to all counsel of record.

/s/Michael W. Seitz
Attorney for Plaintiffs